KIBER JINOYATCHILIKNING YANGI SHAKLLARI VA ULARNI HUQUQIY BAHOLASH

Parvina G‘ulomamatova
Toshkent davlat yuridik universiteti
Kiber huquq kafedrasi
O‘qtuvchisi.
Eshmanov Sardor Salim o’ g’ li
Toshkent davlat yuridik universiteti
Xalqaro huquq va qiyosiy huquqshunoslik fakulteti
2-kurs talabasi
sardoreshmamon96@gmail.com.

Anotatsiya: Ushbu maqolada zamonaviy raqamli texnologiyalarning keng qo;llanilishi natijasida yuzaga kelayotgan kiber jinoyatchilikning yangi shakllari, ularning xususiyatlari va jamiyatga tahdidlari tahlil qilinadi. Ayniqsa, fishing, ransomware, identifikatsiya o’g’riligi, ijtimoiy muhandislik (social engineering) kabi jinoyat turlari misolida ularning kengayib borayotgan ko’lami yoritilgan. Shuningdek, ushbu jinoyatlarga nisbatan milliy va xalqaro huquqiy mexanizmlarning mavjud holati, ularning yetarliligi va dolzarb muammolari yoritilib, huquqiy baholash mezonlari ko’rib chiqilgan. Maqola so’ngida kiber jinoyatchilikka qarshi samarali kurash choralarini ishlab chiqish bo’yicha taklif va tavsiyalar berilgan.

Kalit so‘zlar: kiber jinoyatchilik, raqamli xavfsizlik, fishing, ransomware, ijtimoiy muhandislik, huquqiy baholash, xalqaro huquq, axborot texnologiyalari, kiber xavfsizlik, jinoyat kodeksi.

New forms of cybercrime and their legal assessment

Annotation: This article analyzes new forms of cybercrime arising as a result of the widespread use of modern digital technologies, their characteristics and threats to society. In particular, the expanding scope of such crimes as phishing, ransomware, identity theft, social engineering is highlighted. Also, the current state of national and international legal mechanisms in relation to these crimes, their adequacy and current problems are highlighted, and the criteria for legal assessment are considered. At the end of the article, proposals and recommendations are given for the development of effective measures to combat cybercrime.

Keywords: cybercrime, digital security, phishing, ransomware, social engineering, legal assessment, international law, information technologies, cyber security, criminal code.

Новые формы киберпреступности и их правовая оценка

Аннотация: В данной статье анализируются новые формы киберпреступности, возникающие в результате широкого использования современных цифровых технологий, их характеристики и угрозы для общества. В частности, выделяется расширяющаяся сфера таких преступлений, как фишинг, программы-вымогатели, кража личных данных, социальная инженерия. Также выделяется современное состояние национальных и международных правовых механизмов в отношении этих преступлений, их адекватность и актуальные проблемы, рассматриваются критерии правовой оценки. В конце статьи даются предложения и рекомендации по разработке эффективных мер борьбы с киберпреступностью.

Ключевые слова: киберпреступность, цифровая безопасность, фишинг, программы-вымогатели, социальная инженерия, правовая оценка, международное право, информационные технологии, кибербезопасность, уголовный кодекс.

Kirish(Introduction)

Bugungi kunda raqamli texnologiyalarning rivojlanishi axborot va shaxsiy ma’lumotlarning qayta ishlashni yuqori bosqichlarga olib chiqmoqda. Axborot kommunikatsiya texnologiyalarining rivojlanishi bir tomondan qulaylik va ko‘ plab afzalliklarga olib kelsa, boshqa tomondan aholi o’rtasida kiber jinoyatlarning soni ortib borishiga sabab bo’lmoqda. Bu kabi holatlar oddiy aholining shaxsi, uning shaxsiy ma’lumotlari hattoki mol-mulki kiber jinoyatlarning obyektiga aylanib qolishiga sabab bo’ladi. Internet tarmoqlari bugun dunyoning istalgan nuqtasida mavjud va undagi bajarib bo’lmaydigan ishlarning soni juda kam. Shaxsning birgina qidiruviga o’nlab javoblar topiladi. Kiber olamning cheksizligi kiberjinoyatchilikning ham soni qanchalik ko‘ pligidan dalolat beradi.

Ushbu tahliliy ish orqali kiber jinoyatlar va ularning yangi-yangi shakllari, kiber jinoyatlarning keltirib chiqarayotgan asosiy omillar, kiber jinoyatchilikning tashqi belgilari va ulardan huquqiy himoyalanish mexanizmlari hamda kiberinoyatchilikka qarshi kurashish bilan bog’liq jihatlarni tahlil qilamiz. Shuningdek, kiber jinoyatchilikning oldini olishda milliy hamda xalqaro qonunchilikka asoslanish, mavjud milliy va xalqaro huquqiy hujjatlarning zaruriyatini asoslashga, kiber-tahdidlarning milliy va xalqaro huquqiy oqibatlarini batafsil o‘ rganishga harakat qilamiz.

Metodlar (Methods)

Kiber jinoyatlarning yangi shakllari va ularning huquqiy baholashning umumiy jihatlarini quyidagilar orqali tahlil qilamiz:

1.**Zaruriy manbalar tahlili:** maqolalar, normativ huquqiy hujjatlar, mavzuga oid ilmiy-nazariy adabiyotlar va ma’lumotlarni har tomonlama ko’rib o’rganish tahliliy

ishimizning asosini tashkil qiladi. Bundan tashqari xalqaro va milliy qonunchilik normalarini o'rganish orqali mavjud qonunchilikdagi kamchiliklarni aniqlash.

2.**Case study metodi**: kiber jinoyatlarning turlari va shakllarini turli amaliy misollar, kiberjinoyatlarga oid sud qarorlari va turli davlatlar tajribasini tahlil qilish orqali mavzuni chuqurroq o'rganishga harakat qilamiz.

3.**Qiyosiy huquqiy tahlil**: bugungi kunda butun dunyoda kiberxavfsizlik sohasidagi olib borilayotgan ishlar, davlatlarning keyingi rivojlanish bosqichidagi kiberjinoyatchilikning va kiberxavfsizlikni ta'minlashning o'rni va rolini tahlil qilamiz. O'zbekiston Respublikasi hududida va boshqa rivojlangan davlatlar, jumladan AQSH, Rossiya federatsiyasi, Xitoy davlatlarida mavjud holatlarni qiyoslash va taqqoslash orqali o'rganamiz.

Natijalar(Results)

Nazariy ma'lumotlar, normativ huquqiy hujjatlarni o'rganish, amaliy misollar orqali tahlil qilamiz. Tahlil natijalariga ko'ra kiberjinoyatchilikning yangi shakllari, ularning rivojlanish dinamikasi, xalqaro huquqiy me'yorlar orqali taqqoslash yo'li bilan O' zbekiston qonunchiligidagi mavjud kamchiliklar va qiyosiy huquqiy tahlil asosida aniqlangan muhim jihatlarni o'z ichiga oladi.

Tahlilimiz davomida so'nggi yillarda keng tarqalgan va rivojlanayotgan kiberjinoyatchilik shakllari aniqlab chiqildi:

11. **Sun' iy intellekt yordamida sodir etilayotgan hujumlar**: Kiberjinoyatchilar sun'iy intellektdan foydalanib, himoyalangan tizimlarga buzib kirish, avtomatlashtirilgan fishing hujumlarini amalga oshirish kabi ko' plab yangi-yangi usullarni qo' llab sodir etilayotgan jinoyatlar
12. **Shaxsiy ma' lumotlardan noqonuniy foydalanish**: qulay va tez ma' lumot ulashish imkoniyati o' z navbatida yangi turdagi kiber jinoyatlar xavfini keltirib chiqaradi. Ayniqsa shaxsga doir ma' lumotlarni tez tarqalishi kiber tahdidlar xavfini ham yana kuchayishiga sabab bo' ladi.
13. **Deepfake texnologiyalari yordamida sodir etilayotgan jinoyatlar**: Sun'iy intelekt yordamida soxta audio va videomateriallarni yaratish va bu texnologiyalardan davlat arboblarini umuman olganda barcha shaxslarni obro' sizlantirish, firibgarlik va tovlamachilik kabi g' arazli maqsadida foydalanilmoqda. Masalan, 2020-yilda Britaniyada sodir etiilgan holat yuzasidan bir yirik kompaniyasi deepfake orqali tuzilgan

soxta audiolar yordamida 250 ming funt sterling miqdorida mablag‘ ni yo‘ qotgan.[1]

14. **Kriptovalyutalar orqali firibgarlik va pul yuvish**: Kriptovalyutalar tranzaksiyalarni anonim tarzda amalga oshirish imkoniyatini bergani sababli, ko‘ plab noqonuniy faoliyatlarda ishlatilib kelinmoqda. Bitkoinlar orqali noqonuniy tranziksiyalar soni yangi jinoyat turi sifatida yildan yilga oshib bormoqda.

Tahlil natijasida shuningdek, O’zbekiston qonunchiligida kiberjinoyatchilik bo’yicha mavjud holat va uning kamchiliklari, kiberjinoyatchilikka qarshi kurash bo’yicha asosiy normativ huquqiy hujjatlar: O’zbeksiton Respublikasi Konstitutsiyasi, O’zbeksiton Respublikasi Jinoyat kodeksi, Kiberxavfsizlik to’g’risidagi qonunlar ijrosi yuzasidan tahlillarni keltirib o’tamiz.

Muhokama(Discussion)

Bugungi kun texnologiya davrida texnologiyaning jadal rivojlanishi bevosita inosonlar ongining ham sezilarli o‘ zgarishiga sabab bo‘ lmoqda, bu esa texnologiya bilan bog‘ liq sodir etiladigan jinoyatlarning ham murakkablashib borishiga o‘ z ta’ sirini ko‘ rsatadi. Internet foydalanuvchilar sonining yildan yilga o‘ sib borishi va unga mukkasidan ketish holatlari real xavf – kiber jinoyatlarni keltrib chiqarmoqda. Texnologik yutuqlar vaqt hamda masofa jihatidan yutuq biroq ular oqibatidagi kiber jinoyatlar esa inson hayotiga real tahdid. Bu kabi holatlar esa huquqiy tartibga solish asoslarini yaratishni, har bir kiber hujum yohud texnologik olamda sodir etilgan shaxs manfaatlariga zid bo‘ lgan qilmishlarga yarasha javob qaytarilishini taqozo etmoqda. Shu sababli davlatlar va xalqaro tashkilotlar tomonidan axborot xavfsizligini ta’ minlash, kiberjinoyatchilikka qarshi samarali chora-tadbirlarni ishlab chiqish hamda huquqiy tartiblarini yaratish orqali kiber tahdidlarga qarshi kurashish maqsad qilingan.

Qonunchilik

1) O‘ zbekiston Respublikasi Konstitutsiyasi (33-modda);
2) O‘ zbeksiton Respublikasi Jinoyat kodeski(XXI bob);
3) O‘ zbekiston Respublikasining Ma’ muriy javobgarlik to‘ g‘ risida kodeksi;
4) “ Kiberxavfsizlik to‘ g‘ risida” gi O‘ zbekiston Respublikasi qonuni;
5) O‘ zbekiston Respublikasining “ Shaxsga doir ma’ lumotlar to‘ g‘ risida” gi 547-son qonuni;
6) 2022-yildagi “ Elektron hujjat aylanishi to‘ g‘ risida” gi qonun yangi tahriri, raqamli hujjatlar xavfsizligini himoyasi bilan bog‘ liq.

[1] Robert M. Chesney, Computer Network Operations and U.S. Domestic Law: An Overview, 89 INT’L L. STUD. 218, 230□32 (2013).

Nazariy va amaliy tahlil

Kiberjinoyatchilik - axborotni egallash, uni o‘ zgartirish, yo‘ q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’ minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘ indisi.[2]

Kiberjinoyatlar odatda tarmoq hamda kompyuter axborot tizimlariga hujumlar, shaxsiy ma’ lumotlarni o‘ g‘ irlash va ulardan noqonuniy foydalanish, zararli dasturlarni tarqatib yuborish, moliyaviy hujumlar va firibgarlik kabi qilimishlarni o‘ z ichiga oladi. Kiberjinoyatchilik, kiberqonunlar hamda kibernetika global miqyosdagi dolzarb masala bo‘ lganligi sababli ko‘ plab olimlar tomonidan ushbu yonalishda ilmiy ish va maqolalar yozilgan, rasmiy hisobotlar tayyorlangan. Bularning barchasi muammolarning yechimi uchun nazariy va amaliy bilimlarni taqdim qiladi. Bularga misol qilib ***D.S.Wall*** tomonidan (2007) yozilgan “*Cybercrime: The Transformation of Crime in the Information Age*” asarini olsak, unda aynan biz tahlil qilishimiz kerak bo‘ lgan jihatlar – kiberjinoyatlarning shakllari va ularning bugungi zamonaviy dunyoga ta’ siri batafsil yoritib berilgan.

Kiberjinoyatning ta’siri haqida ilgari ko□plab asossiz da’volar bo‘lsa-da, bugun hukumatlar, politsiya, agentliklar va kiberxavfsizlik tashkilotlari kiberjinoyatlarga javob berishda, ularning oldini olish va tekshirishda ko‘proq mahorat va tajribaga ega bo‘ldi. Ular shaxsiy kiberxavfsizlikni kuchaytirish maqsadida milliy va xalqaro kiberxavfsizlik siyosatini rivojlantirish choralarini ko‘rishmoqda biroq bularning o‘ zi yetarli emas. Tashkilotlar rivojlanishda biroz oldiga siljishlar bo‘ lishiga qaramasdan muammolarga to‘ liq javob hamda yechim berish qobiliyatiga ega emas. Muammo shundaki, kiber jinoyat, xuddi firibgarlik kabi, *“ portlamaydi, qon oqmaydi yoki qichqirmaydi”* (Buyuk Britaniya politsiyasining yuqori lavozimli vakilidan iqtibos) shuning uchun huquqbuzarlikning zo'ravonlik shakllariga berilgan siyosiy ustuvorlikni ololmaydi. Shu bilan birga, kiberjinoyatlar nima ekanligi va ular qanday ta'sir qilishi haqida tushunmovchiliklar jamiyat orasida hali hamon saqlanib qolmoqda.[3]

Kiberxavfsizlikni ta’ minlash nafaqat shaxslar huquqlari himoyasi balki butun mamlakatlarning xavfsizligi va iqtisodiy farovonligi uchun muhim ahamiyatga ega. Axborotlar xavfsizligi va internet aloqa vositalariga hujumlar soni kundan kunga oshib borishi esa haqiqiy tashvishli jihat. Bulardan onlayn firibgarlik va xakkerlik hujumlari har kuni sodir etiladigan kiberjinoyatlarga kichik bir misol bo‘ la oladi. Keling kiberjinoyatchilik bilan bog‘ liq rasmiy *statistik ma’ lumotlarni* tahlil qilib o‘ tamiz. 2003-yilning o‘ zida kiberjinoyatchilik natijasida yetkazilgan zararning miqdori 32

[2] https://lex.uz/uz/docs/-5960604 □Kiberxavfsizlik to‘ g‘ risida□gi O‘ zbekiston Respublikasi qonuni

[3] https://www.researchgate.net/profile/David-Wall7/publication/378013252_Cybercrime_The_Transformation_of_Crime_in_the_Information_Age_2nd_edition/links/65c36f3179007454976a5420/Cybercrime-The-Transformation-of-Crime-in-the-Information-Age-2nd-edition.pdf

milliard dollarga yetgan. Boshqa hisob-kitoblarga ko‘ ra esa 2007-yilga kelib kiberjinoyatchilikdan olingan daromadlar miqdori hattoki narkotrafikani ortda qoldirgan va 100 millliard AQSH dollariga yetgan. Bu juda katta raqamlarni tashkil qiladi. 2014-yilgi tadqiqotlar esa kiberjinoyatchilikdan yo‘ qotishlarning umumiy miqdori bir yilda 400 milliard dollarga yetganini ko‘ rsatadi. Bu raqamlar axborot infratuzilmalarini himoyasini ta’minlashning haqiqiy zaruriyatini isbotlab turibdi. Bugunga kelib esa har 1 daqiqada taxminan 100000dan ortiq hujumlar aniqlanmoqda.[4]

Yuqorida qayd etilgan hujumlarning aksariyati muhim infratuzilmalarga qaratilgan bo‘ lmasligi mumkin, ammo 2010-yilda topilgan “ Stuxnet” nomli zararli dastur 37 ta infratuzilmaga qaratilgan hujumlar xavfini ko‘ rsatadi. Ushbu dasturiy vosita foydalaniladigan dasturlarni 4000dan ortiq funksiyalari zararlangani qayd etilgan.[5]

Kiber jinoyat tushunchasiga quyidagicha tasnif berishimiz mumkin – “ qasddan jinoiy niyat bilan shaxs yoki bir qancha shaxslar guruhiga nisbatan sodir etilgan qilmish. Ushbu jinoyat natijasida bevosita yoki bilvosita jabrlanuvchiga jismoniy hamda ruhiy zarar yetkazilgan bo‘ lishi, yo‘ qotishlarga sabab bo‘ lishi, jabrlanuvchining obro‘ si va qadr qimmatiga putur yetkazadigan bo‘ lishi mumkin” . Kiber jinoyat davlatning tinchligiga va moliyaviy xavf tug‘ dirish, mualliflik huquqlari buzilishi, bolalar pornografiyasi, kiber taqib qilish, kiber tuhmat , polimorf virus kabi shakllarda bo‘ ladi. Shuningdek, ***Debarati Xolder va K.Jaishankar*** kabi tadqiqotchilarning fikriga ko‘ ra esa gender nuqtai nazaridan yuqoridagi shakllarga qo‘ shimcha ravishda “ *ayollarga qarshi kiber jinoyat*” turi ham alohida takidlangan. Bunga sabab, bugungi kunda tarmoqlar orqali ayollarga nisbatan psixologik hamda fiziologik tazyiq o‘ tkazish motivini yaratish holatlari, ayollarga qarshi jinoyatlar soni oshib borayotgani edi. Bunda ayol tarmoqlar orqali nishonga olinadi, uning shaxsiy ma’ lumotlari olinadi qayta ishlanib yolg‘ on axborotga aylantirib ayolning shani qadr-qimmatiga zarar yetkazadigan tarzda talqin qilinadi. Bundan tashqari ko‘ plab holatlar bo‘ lishi mumkin, mo‘ may daromadli ish taklif qilish, arzon haridlar, foydali niqobi ostidagi reklamalar orqali kiberjinoyatchilik qurboniga aylantirib qo‘ yishadi.

Yuqoridagilardan ushbu jinoyat turi faqatgina ayollar o‘ rtasidagina sodir etiladi degan xulosaga kelib qolmasligimiz kerak. Kiber jinoyat turli yoshdagi shaxslarga turli hil asoslar bilan sodir etiladi. Quyida ayrim xususiyatlarni ko‘ rib tahlil qilib o‘ tamiz:

1)***Yosh bilan bog‘ liq xavf omillari***. Kiber jinoyatlarning qurboni bo‘ layotganlarning asosiy qismini 60 yoshdan yuqori shaxslar tashkil qilar ekan.

[4] Yevropa Kengashi - Kompyuter jinoyatchiligi to‘g‘risidagi konvensiyasi axboroti (№ 185)(Budapest, 23-noyabr 2001-yil)

[5] Yevropa Kengashi - Kompyuter jinoyatchiligi to‘g‘risidagi konvensiyasi axboroti (№ 185)(Budapest, 23-noyabr 2001-yil)

Ixtiyoridagi mablag‘ larni himoya qila olmasliklari sababli firibgarlik va moliyaviy hujumlarni o‘ ljasiga aylanib qolishadi. Shuningdek mutaxasislarning fikriga ko‘ ra ushbu yoshdagi shaxslarda internet va aloqa vositalaridan foydalanish ko‘ nikmalari yetarli emas va ayrimlari esa umuman tanish emas. 25 yoshgacha bo‘ lganlar texnologiyalardan foydalanishni bilishadi, bugungi kiber tahdidlardan habardor bo‘ lishsa ham o‘ z manfaatlarini himoya qilish tajribasi yo‘ q. Ular bilan sodir bo‘ lishi mumkin bo‘ lgan holatlarni oldini olish choralarini ko‘ rishmaydi, “ kiber hujumlar men bilan sodir bo‘ lishi mumkin emas” deb hisoblashadi.

2)***Umumiy xavflar*** ya’ ni kiberxavfsizlik qoidalariga amal qilmagan har qanday yosh va kasbdagi shaxslar kiber jinoyat qurboni bo‘ lishi mumkinligini nazarda tutilmoqda. Birgina zaif parollar o‘ rnatilishining oqibatida ham ko‘ plab kiber jinoyatlarga yo‘ l ochib berilishi mumkin. Bir qurilmaga o‘ rnatilgan parollarning boshqa qurilmalarga mos kelishi birgina parol orqali butun raqamli hayotingizga begona shaxslarning kirishi huquqini berishi mumkin.[6]

O‘ zbekiston Respublikasi qonunchiligiga ko‘ ra yuqoridagi kabi kiber jinoyatlar uchun javobgarlik aoslari belgilab qo‘ yilgan.

Birinchi navbatda **O‘ zbekiston Respublikasi Konstitutsiyasi 33-moddasiga** asosan davlat Internet jahon axborot tarmog‘ idan foydalanishni ta’ minlash uchun shart-sharoitlar yaratadi. Axborotni izlash, olish va tarqatishga bo‘ lgan huquqni cheklashga faqat qonunga muvofiq hamda faqat konstitutsiyaviy tuzumni, aholining sog‘ lig‘ ini, ijtimoiy axloqni, boshqa shaxslarning huquq va erkinliklarini himoya qilish, jamoat xavfsizligini hamda jamoat tartibini ta’ minlash, shuningdek davlat sirlari yoki qonun bilan qo‘ riqlanadigan boshqa sir oshkor etilishining oldini olish maqsadida zarur bo‘ lgan doirada yo‘ l qo‘ yiladi.[7]

O‘ zbeksiton Respublikasi Jinoyat kodeksida ham kompyuter texnologiyasidan foydalanib sodir etilgan jinoyatlarga nisbatan javobgarlik choralari belgilab qo‘ yilgan. Jinoyat kodeksida nazarda tutilgan 38 ta jinoyat tarkibida, ya’ ni 7,7% holatda kompyuterdan vosita sifatida foydalanib sodir etilgan jinoyatlar tashkil etar ekan. Ushbu jinoyatlarni obyektiga nisbatan shartli ravishda quyidagi turlarga ajratishimiz mumkin:

1) kompyuter vositasidan foydalanib, oilaga, yoshlarga, axloqqa qarshi qaratilgan jinoyatlar;
2) kompyuter vositasidan foydalanib, shaxsning ozodligi, shani, qadr-qimmatiga qaratilgan jinoyatlar;
3) kompyuter vositasidan foydalanib, fuqaroning konstitutsiyaviy huquq va erkinliklariga qarshi qaratilgan jinoyatlar;

[6] Карпова Д.Н. Киберпреступность: глобальная проблема и её решение. //Власть. №8. 2014. С. 46-50
[7] https://lex.uz/docs/-6445145#-6445676

4) kompyuter vositasidan foydalanib, O‘ zbekiston Respublikasiga qaratilgan jinoyatlar;
5) kompyuter vositasidan foydalanib, o‘ zgalar mulkini talon-taroj qilish jinoyati;
6) kompyuter vositasidan foydalanib, iqtisodiyot asoslariga qarshi qaratilgan jinoyatlar;
7) kompyuter vositasidan foydalanib, boshqaruv tartibiga qarshi jinoyatlar;
8) kompyuter vositasidan foydalanib, odil sudlovga qarshi jnoyatlar;
9) kompyuter vositasidan foydalanib, jamoat xavfsizligi va jamoat tartibiga qarshi jinoyatlar.[8]

Kiberjinoyatchilikka oid normalarning qanchalik qat’ iy belgilab qo‘ yilgan bo‘ lmasin bugungi texnologik o‘ sish ushbu qonunchilikni qayta ko‘ rib chiqishni talab etmoqda. Shuni ham alohida takidlash joizki, bugungi kunda dunyoning100 dan ortiq davlatlari, jumladan Interpol a’ zolarining 60%ida kiberjinoyatchilikka qarshi kurashish uchun qabul qilingan qonunlar mavjud emas.[9]

Butun dunyoda kiberxavfsizlik sohasi kuchaygan davrda boshqa davlatlar tajribasinni o‘ rganish, amaliy jihatlarini o‘ z mamlakatimizda tadbiq etish juda muhim. Shu jihatdan ***Rossiya federatsiyasi*** misolida olsak, voyaga yetmaganlar uchun ushbu davlatda alohida internet tarmog‘ i yaratilgan ekan, ***Xitoy davlati*** esa voyaga yetmaganlar uchun internetdan foydalanish soatlari tartibini joriy etgan, ayrim davlatlarda (**Hindiston)** jamiyat rivojlanishi uchun to‘ sqinlik qiladigan saytlarga cheklovlar o‘ rnatilgan.

Axborotlashtirish va kompyuter jinoyatlari sohasida qabul qilingan ilk normativ huquqiy hujjat ham 1978-yilda AQSHda qabul qilingan bo‘ lib ***“ Kompyuter jinoyatlariga qarshi akt” [10]***. Ushbu huquqiy hujjatni qabul qilinishi AQSHning ushhbu yo‘nalishda ancha oldinda ekanini isbotlab turibdi.

AQSH qonunchiligi va bizdagi kabi kiber jinoyatlar yagona huquqiy hujjatlar bilan tartibga solingan bo‘ lib, Buyuk Britaniyada esa bundan farqli ravishda alohida-alohida qabul qilingan qonun hujjatlari bilan javobgarlik belgilanadi. Masalan, ***“ Jinsiy jinoyatlar to‘ g‘ risida***”[11]gi qonunga ko‘ ra 16 yoshga to‘ lmagan bolalarga pornografik mahsulotlar tarqatgan shaxslarga joniy javobgarlik belgilangan.

Raqamli texnologiyalar global miqyosda rivojlanar ekan, kiber jinoyatlar ham hudud bo‘ yicha kengayib, transmilliy tus olib boraveradi. Bugungi kunda bitta davlat doirasida kiberxavfsizlikni ta’ minlashning o‘ zi yetarli emas, chunki aksariyat kiberhujumlar boshqa davlatlardan boshqariladi yoki ularda sodir etiladi. Masofadan

[8] Salayev.N.S., Ro‘ziyev.R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya // Ma’sul muxarrir: y.f.d.,prof. R.A.Zufarov. – Toshkent: TDYU,2018. – 139 bet.
[9] https://www.gazeta.uz/ru/
[10] F.I. Computer crimes Act tit. XLVI Chapter 815 (1978)
[11] Sexual Offences Act 1956

turib tahdidlar amalga oshirish hozir keskin tus olgan. Shu sababli, xalqaro hamkorlik kiberjinoyatchilikka qarshi kurashishda hal qiluvchi rol o‘ynaydi. Kiberjinoyatchilikka qarshi samarali kurashish biror davlatning yakkama-yakka harakati bilangina erishilmaydi, balki keng ko‘lamli xalqaro hamkorlik asosida amalga oshiriladi. Shu sababli, O‘zbekiston ham Budapesht konvensiyasi va boshqa xalqaro shartnomlarga qo‘shilishi, xalqaro axborot almashinuvi tizimlariga integratsiyalashuvi va xalqaro tashkilotlar faoliyatida faol ishtirok etishi, ilg‘or tajribalarni mamlakat hududida joriy etilishi orqali kiberxavfsizlikni yanada mustahkamlashi mumkin.

Xulosa

Kiberxavfsizlikni ta’minlash, foydalanuvchilarning himoyasi nafaqat butun hukumatning balki boshqa tashkilotlarning ham asosiy vazifasi. Davlat o‘z hududidagi fuqarolarning huquqlarini himoya qilish, baxtsiz hodisalarning oldini olishi va ularni bartaraf etish choralarini ko‘rishi zarur. Kiberjinoyatchilikka qarshi kurashish uchun har bir davlat kiberxavfsizlikni to‘g‘ri tashkil qilishi va himoya mexanizmlarini ishlab chiqishi zarur. Bu borada davlatlar o‘rtasidagi xalqaro hamkorlikni rivojlantirish ham juda muhim. Kiberjinoyatlar asosan rivojlangan va rivojlanayotgan davlatlar hududida sodir etiladi. Bunga sabab yirik ishlab chiqarish korxonalari, katta kompaniyalar va banklar ushbu davlatlarda, bu esa kiberjinoyatlar uchun mo‘may gina daromad manbayi bo‘la oladi. Bunday holatlarni oldini olish uchun esa davlat birinchi navbatda axborot texnologiyalarini jinoiy maqsadlarda va boshqa g‘ayriqonuniy faoliyatlarda foydalanishga qarshi tegishli qonun hujjatlarini qabul qilishi lozim. Birgina normativ asoslarni yaratishning o‘zi ham bu borada foyda bermasligi mumkin. Shuning uchun kiberxavfsizlikni ta’minlash, kiberjinoyatchilik shakllarini yanada ko‘payishi oldini olish uchun kompleks yondashuv lozim. O‘zbekistonda ham kiberxavfsizlikni ta’minlash uchun huquqiy asoslar mavjud bo‘lsada, mavjud qonunlarni yanada takomillashtirish va ilg‘or xorijiy tajribalarni joriy qilish lozim. Xalqaro hamkorlik hamda tajriba almashinuvi kiber jinoyat shakllariga qarshi kurashda muhim rol o‘ynaydi.

Texnik chora-tadbirlarni amalga oshirish bilan bir qatorda huquqni muhofaza qiluvchi organlarning kiberjinoyatchilikni samarli tarzda tekshirish va jazolash tizimini shakllantirish kerak. Aholining huquqiy ongi va madaniyatini oshirish, internet tarmoqlaridan foydalanish madaniyatini shakllantirish, barcha ta’lim muassasalarda, ish joylarida kiberjinoyatlarda ogohlantirish choralarini ko‘rish ham kiberxavfsizlikni ta’minlashda muhim ahamiyatga ega.

Xulosa sifatida kiber jinoyatlarning oldini olish va kiberxavfsizlikni takomillashtirish uchun quyidagi quyidagilarni amalga oshirish lozim deb hisoblayman:

huquqiy asoslarni mustahkamlash – milliy qonunchilikni xalqaro standartlarga moslashtirish, kiberjinoyatchilik bo‘ yicha maxsus qonun qabul qilish hamda mavjudlarini takomillashtirish;

huquq-tartibot organlarini rivojlantirish – kiberjinoyatchilikka qarshi kurashish bo‘ yicha maxsus bo‘ linmalar tashkil etish;

fuqarolarning xabardorligini oshirish – jismoniy hamda yuridik shaxslar uchun kiberxavfsizlik bo‘ yicha dasturlar ishlab chiqish, huquqiy savodxonlik hamda texnologik bilimlari oshirish choralarini korish;

yangi texnologik yutuqlarni kiberxavfsizlk yonalishida ham joriy etish – kiberxavfsizlik tizimlarini takomillashtirish, sun’ iy intellektdan huquqni muhofaza qilish tizimlarida keng foydalanish.

Ushbu choralar kiber makonda xavfsiz muhit yaratish uchun hizmat qiladi. Kelajakdagi sodir etilishi mumkin bo‘ lgan kiber jinoyatlarning yangi shakllarini oldini olishga yordam bera oladi.

Foydalanilgan adabiyotlar:

1. O’zbekiston Respublikasi Konstitutsiyasi;
2. O’zbeksiton Respublikasi Jinoyat kodeski;
3. O’zbekiston Respublikasining Ma’muriy javobgarlik to’g’risida kodeksi;
4. Kiberxavfsizlik to’g’risidagi O’zbekiston Respublikasi qonuni;
5. O’zbekiston Respublikasining Shaxsga doir ma’lumotlar to‘g‘risida”gi 547-son qonuni;
6. Salayev.N.S., Ro‘ziyev.R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya // Ma’sul muxarrir: y.f.d.,prof. R.A.Zufarov. – Toshkent: TDYU,2018. – 139 bet;
7. Карпова Д.Н. Киберпреступность: глобальная проблема и её решение. //Власть. №8. 2014. С. 46-50;
8. Robert M. Chesney, Computer Network Operations and U.S. Domestic Law: An Overview, 89 INT’L L. STUD. 218, 230–32 (2013).
9. “Cybercrime: The Transformation of Crime in the Information Age” D.S.Wall (2007);
10. Yevropa Kengashi - Kompyuter jinoyatchiligi to‘g‘risidagi konvensiyasi axboroti (№ 185)(Budapest, 23-noyabr 2001-yil);