ISSN 2181-3187

KIBER HUQUQIY MASALALARNI VA ULARNI HAL QILISH BO'YICHA XORIJIY TAJRIBA

Raximjanova Tursunoy
Tashkent state university of law, Faculty of international law and comparative law
Email: tursunoyraximjon@gmail.com

Abstract. Cyber-crime is increasing day by day in today's information technology society. For this reason, it is difficult to regulate crime that occurs on this online platform based on the criminal legislation that was in force several decades ago. For this reason, there is a demand for new legislation to prevent this crime and punish it based on the law. For this, the use of the experiences of foreign countries is of great importance. Nowadays, many people do not have a clear understanding of what cybercrime is. The question of the concept of cyber-crime and its types is something that makes people think. This article discusses information on the above issues and examines the experience of international countries within the framework of cybercrime.

Keywords: Cybercrime, online platform, experiences of foreign countries, cyber space.

Anotatsiya. Bugungi axborot texnologiyalar rivojlangan jamiyatda kiber jinoyatchilik kundan kunga ko'payib bormoqda. Shu sababli bir necha o'n yilliklar avval amalda bo'lgan jinoyat qonunchiligi asosida ushbu online platformada sodir bo'ladigan jinoyatchilikni tartibga solish mushkul hisoblanadi. Shu sababli ushbu jinoyatchilikni oldini olish, qonunchilik asosida jazoga tortish uchun yangi qonun hujjatlariga talab vujudga keladi. Buning uchun esa xorijiy davlat tajribalaridan foydalanish juda katta ahamiyat kasb etmoqda. Hozirgi kunda ko'pchilikda kiberjinoyatchiliknima ekanligi haqida aniq tushuncha mavjud emas. Kiber jinoyatchilik tushunchasi va uning qanday turlari borligi masalasi insonni o'ylantirishi turgan gap. Ushbu maqolada yuqoridagi masalalar yuzasidan ma'lumotlar muhokama qilinadi va kiberjinoyatchilik mavzusi doirasida xalqaro mamlakatlar tajribasi ko'rib chiqiladi.

Kalit so'zlar: kiberjinoyat, online platforma, xorijiy mamlakatlar tajribasi, kiber makon.

Kiberjinoyatchilik tushunchasi

Kiber jinoyat tushunchasi haqida O'zbekiston Respublikasi Kiberxavfsizlik to'g'risidagi qonuning 3-moddasida ma'lumot berib o'tilgan. Unga ko'ra **kiberjinoyatchilik**- axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot

ISSN 2181-3187

va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig'indisi hisoblanadi. Umuman olganda kiberjinoyat raqamli qurilmalar va tarmoqlar yordamida amalga oshiriladigan jinoiy harakatlardir. U komputer tizimlari, tarmoqlar va online platformadagi zaifliklardan foydalanadigan keng ko'lamli noqonuniy harakatlarni o'z ichiga oladi. Kibermakon ya'ni axborot texnologiyalari yordamida yaratilgan virtual muhitda sodir etiladigan jinoyatlarning bir necha turlari mavjud. Quyida ularning keng tarqalgan turlaridan ba'zilari keltirilgan:

1. **Identity theft,** ya'ni identifikatsiyani o'g'irlash. Bunda kimdir nomini o'zgartirish yoki ruxsatsiz tranzaksiyalarni amalga oshirish uchun parollar, kredit karta raqamlari yoki ijtimoiy xavfsizlik raqamlari kabi shaxsiy ma'lumotlari o'g'irlanadi.
2. **Fishing**- oshkor qilish mumkin bo'lmagan ma'lumotlarni oshkor qilish va zararli dasturlarni yuklab olish uchun shaxsni aldash maqsdida turli xil soxta elektron pochta yoki xabarlarni yuborish.
3. **Kiber bulling**- ijtimoiy media, xabar almashish ilovalari yoki boshqa raqamli platformalar orqali onlayn platformalar orqali shaxslarni ta'qib qilish, qo'rqitish yoki tahdid qilish.
4. **Kiberjosuslik**- siyosiy, iqtisodiy yoki harbiy maqsadlarda hukumatlar, korxonalar yoki jismoniy shaxslarning maxfiy ma'lumotlari yoki intellektual mulkiga noqonuniy kirish va o'g'irlash jinoyatlari hisoblanadi.

Kiberjinoyat bu aynan bir davlat hududida bo'ladigan yoki aynan bir davlat hududi doirasiga tegishli muammo emas. Ushbu jinoyat butun dunyo uchun hal qilinishi yoki chora ko'rilishi kerak bo'lgan muhim masalalar qatoridan o'rin oladi. Bu holatda mamlakatlar kiberjinoyatchilik sohasi yuzasidan xalqaro hamkorlik olib borishni muhokama qilishlarini talab etadi. Hozirgi kunda bir davlat hududida bo'lib boshqa bir davlat hududidagi insonga kiber hujum uyushtirish holatlari ajablanarli holat emas. Ya'ni bugungi kun voqeiligi bilan aytganda ushbu holat odatiy holga aylanib qolgan. Kiberjinoyatchilikning chegarasi davlatning chegarasi tugagan joyda to'xtaydi degan fikr mutlaqo xato hisoblanadi.

Kiberjinoyatchilikda yurisdiksiya muammosining so'nggi misollaridan biri "Love Bug" virusi bilan bog'liq. Dunyo bo'ylab milliardlab zarar keltirgan ushbu virus Filippin fuqarosi tomonidan yaratilgan va ishga tushirilgan. Mazkur shaxsning xatti-harakatlari Filippin tergovchilari tomonidan aniqlangan, ammo uning qilmishida Filippinning mavjud moddiy qonunchiligini buzish holati yo'qligi sababli javobgarlikka torta olishmadi. Negaki, Filippinning hakerlik uchun jazo belgilangan "Elektron tijorat to'g'risida"gi qonuni "Love Bug" virusi Internetda paydo bo'lganidan keyin kuchga kirgan. Shunday qilib, ushbu shaxsning xattiharakati virus zarar etkazgan boshqa mamlakatlarda javobgarlikka sabab bo'lgan bo'lsa-da, faqat mazkur shaxs Filippin davlati yurisdiksiyada bo'lganligi sababli, xorij huquq-tartibot idoralari unga nisbatan qidiruv e'lon qilish va jinoiy javobgarlikka tortish masalasini hal eta

ISSN 2181-3187

olmadilar. Hozirgi vaqtda ko‘pgina mamlakatlar o‘zlarining jinoiy qonunchiligini yangiladilar va raqamli jinoyatlarni jazolanadigan jinoyat sifatida o‘z qonunchiligiga kiritib qo‘ydilar[1]. Shuning uchun kiberjinoyatchilikning oldini olish yoki kiberjinoyatchilarni jazolash uchun umumiy ya’ni barcha davlatlar uchun bir xil amal qilishi lozim bo’lgan xalqaro qonun ishlab chiqish lozim. Shunda jinoyatchi qaysi davlat hududida bo’lishidan qat’iy nazar shu qonun orqali javobgarlikka tortiladi.

Kiber huquqiy masalalarni hal qilish bo’yicha tajribalar mamlakat va uning qonunchilik bazasiga ko’ra farq qiladigan jihatlari mavjud. Lekin kiber huquqiy masalalarni hal qilish bo’yicha umumiy bo’lgan yondashuvlar va tendensiyalardan foydalanish mumkin. Ko’plab mamlakatlar kiberjinoyatchilarga qarshi kurashish va kibermakondagi munosabatlarni tartibga solish uchun maxsus qonunlar qabul qilishgan. Ushbu qonunlar xakerlik, identifikatorlarni o’g’irlash, kiberbulling, kiberterorizm va komputer tizimlariga ruxsatsiz kirish kabi huquqbuzarliklarning keng doirasini qamrab oladi. Shu boisdan ham qonunchilik orqali tartibga solish bu kiberchinoyatchilikka qarshi kurashishning asosiy choralaridan biridir. Bundan tashqari ko'pgina mamlakatlarda shaxslarning shaxsiy ma'lumotlarining maxfiyligini himoya qilish va tashkilotlar tomonidan bunday ma'lumotlarni to'plash, saqlash va ulardan foydalanishni tartibga solish uchun qonunlar qabul qilingan. Ushbu qonunlar ko'pincha korxonalarga ular to'playdigan shaxsiy ma'lumotlarni himoya qilish majburiyatlarini yuklaydi va ma'lumotlar buzilgan taqdirda shaxslarni xabardor qiladi.

Kiberjinoyatchilik oqibatida aziyat chekayotgan insonlar ko’rsatkichini kamaytirish maqsadida ushbu soha yuzasidan xalqaro hamkorlik munosabatlarini mustahkamlash lozim. Chunki kiberjinoyatchilik ko’pincha milliy chegaralardan oshib ketadi. Ularga qarshi samarali kurashish uchun mamlakatlar o’rtasidagi hamkorlik zarur. Ayrim mamlakatlar amaliyotida ham ko’rishimiz mumkinki, kiber jinoyatchilarni tergov qilishda yoki aniqlashda ma’lumotlar va dalillar almashinuvini osonlashtirish uchun ikki tomonlama va ko’p tomonlama shartnomalar tuzilgan.

Yana bir muqobil variant sifatida ko’rishimiz mumkin bo’lgan holat bu huquqni muhofaza qilish va sud hokimiyati salohiyatini oshirishdir. Ushbu soha vakillarining kiberjinoyatlarni tergov qilish va javobgarlikka tortish salohiyatini rivojlantirish juda katta ahamiyatga ega. Huquqni muhofaza qilish organlari va sud tizimining xodimlarini o’qitish, kiberjinoyatlarga qarshi kurash bo’yicha ixtisoslashtirilgan bo’limmalarni tashkil qilish, ularni zarur vositalar va resurslar bilan jihozlash maslalalarini yuqoridagi fikr qamrab oladi.

Jamoatchilikning kiberxavflar va onlayn xavfsizligini ta’minlash bo‘yicha ilg‘or amaliyotlar haqida xabardorligini oshirish har qanday kiberhuquqiy bazaning muhim jihati ekanligini jamiyatga yetkazish ham kiberjinoyatchilikning kamaytirish uchun

[1] Abdullayev, Shohzod. "KIBERJINOYATLARNI TERGOV QILISHDA XALQARO-HUQUQIY HAMKORLIK: MUAMMOLAR VA IMKONIYATLAR." Conferencea (2023): 38-49

ISSN 2181-3187

tashlangan katta qadamlardan biri bo’lishi mumkin desak mubolag’a bo’lmaydi. Ushbu soha amaliyotiga shaxslarni kiberjinoyatlarning mumkin bo'lgan oqibatlari haqida ma'lumot berish va ularning raqamli aktivlarini himoya qilish bo'yicha ko'rsatmalar berish kiradi.

Umuman olganda, kiberhuquqiy masalalarni hal qilish qonunchilik, huquqni muhofaza qilish organlari, xalqaro hamkorlik, jamoatchilikni xabardor qilish va salohiyatni oshirishni birlashtirgan ko'p qirrali yondashuvni talab qiladi. Mamlakatlar kibertahdidlar va texnologik taraqqiyotning rivojlanib borayotgan tabiatiga hamqadam bo'lish uchun o'zlarining huquqiy asoslarini doimiy ravishda moslashtirishlari va yangilashlari lozim.

Xalqaro tajriba

Huquqiy tizimlar, madaniy kontekstlar, texnologik infratuzilma va tajriba darajalaridagi farqlar tufayli kiberhuquqiy masalalarni hal qilish ham mamlakatlar o’rtasida farq qiladi. Turli mamlakatlarning kiberhuquqiy masalalarga qanday yondashishiga oid ba'zi keng ko'lamli kuzatishlar ham mavjud:

1. **Amerika Qo‘shma Shtatlari**: Qo‘shma Shtatlarda kiberjinoyatlarga qarshi kurashish uchun keng qamrovli huquqiy baza mavjud, jumladan, kompyuter tizimlariga ruxsatsiz kirishni jinoiy javobgarlikka tortuvchi Kompyuter firibgarlik va suiiste’mol qonuni (CFAA) kiberjinoyatga qarshi asosiy manba hisoblanadi[2]. Bundan tashqari, FQB va Ichki xavfsizlik departamenti kabi agentliklar kiberjinoyatlarni tergov qilish va muhim infratuzilmani kiber tahdidlardan himoya qilishda muhim rol o'ynaydi.

2. **Yevropa Ittifoqi davlatlari**: Yevropa Ittifoqi shaxsiy ma’lumotlarni himoya qilish bo‘yicha qat’iy standartlarni o‘rnatuvchi va talablarga rioya qilmaslik uchun katta miqdorda jarima soladigan umumiy ma’lumotlarni himoya qilish reglamentini (GDPR) qabul qilgan. Evropa Ittifoqiga a'zo davlatlar ham kiberjinoyatchilikka qarshi o'zlarining qonunlariga ega.

3. **Xitoy**: Xitoy kiberjinoyatlarga qarshi kurashish va internet faoliyatini tartibga solish uchun turli qonun va qoidalarni qabul qildi. Xitoyning kiberxavfsizlik qonuni tarmoq operatorlariga foydalanuvchi ma’lumotlarini himoya qilish va kiberxavfsizlik hodisalari haqida xabar berish majburiyatlarini yuklaydi. Mamlakatda, shuningdek, onlayn kontentni nazorat qilish uchun keng qamrovli senzura va kuzatuv choralari qo'llaniladi.

[2] National Association of Criminal Defense Lawyers., accesed April 9, 2024, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

ISSN 2181-3187

4. **Rossiya:** Rossiyada kiberjinoyatlarga qarshi kurash va internetni tartibga solish bo‘yicha qonunlar, jumladan, “Axborot, axborot texnologiyalari va axborotni himoya qilish to‘g‘risida”gi Federal qonun qabul qilindi[3].

5. **Hindiston**: Hindistonda Axborot texnologiyalari to'g'risidagi qonun va Hindiston Jinoyat kodeksi kabi qonunlar bo'lib, ular kiberjinoyatlarning keng doirasini, jumladan, xakerlik, ma'lumotlarni o'g'irlash va onlayn ta'qiblarni qamrab oladi. Mamlakatda, shuningdek, kiber jinoyatlarni tergov qilish va ta'qib qilish uchun Kiber jinoyatlarni tergov qilish bo'limi kabi agentliklar tashkil etilgan.

6. **Yaponiya:** Yaponiyada kiberjinoyatlarga qarshi kurashish va shaxsiy daxlsizlik huquqlarini himoya qilish uchun shaxsiy ma'lumotlarni himoya qilish to'g'risidagi qonun va kompyuterga ruxsatsiz kirishni taqiqlash to'g'risidagi qonun kabi qonunlar mavjud. Mamlakatda kiberxavfsizlikdan xabardorlikni oshirish va hukumat va sanoat manfaatdor tomonlari o‘rtasidagi hamkorlikni rivojlantirish tashabbuslari ham bor.

Yuqorida berilgan misollar davlatlarda amalga oshirilayotgan eng minimal tarzda amalga oshirilgan choralar hisoblanadi. Shu kabi xalqaro tajribalardan foydalangan holatda qonunlar ishlab chiqish va boshqa tadbirlarni amalga oshirish orqali kiberjinoyatchilik ko’rsatkichlarini kamaytirish mumkin.

Xulosa

Yuqoridagi misollar mamlakatlarning kiberhuquq muammolarini hal qilishda ularning o‘ziga xos ustuvorliklari, muammolari va huquqiy an’analarini aks ettiruvchi turli yondashuvlarni ta’kidlaydi. Shu bilan birga, umumiy mavzular qatoriga maxsus qonun hujjatlarini qabul qilish, ixtisoslashgan idoralar tashkil etish, xalqaro hamkorlik va kiberxavfsizlikdan xabardorlik va imkoniyatlarni oshirishga qaratilgan harakatlar kiradi. Umuman olganda Kiberjinoyat butun dunyo bo'ylab jismoniy shaxslar, korxonalar va hukumatlar uchun jiddiy muammolarni keltirib chiqaradi. Chunki u moliyaviy yo'qotishlarga, obro'ga putur etkazilishiga, shaxsiy hayot va xavfsizlikning buzilishiga olib kelishi mumkin. Kiberjinoyatlarga qarshi kurash, uning oldini olish, aniqlash va javob berish strategiyalarini ishlab chiqish uchun huquqni muhofaza qilish idoralari, kiberxavfsizlik bo'yicha mutaxassislar va texnologiya kompaniyalari o'rtasida hamkorlikni talab qiladi.

Foydalanilgan adabiyotlar ro’yxati

1. O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son

2. National Association of Criminal Defense Lawyers., accesed April 9, 2024, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

[3] Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ., accesed April 10, 2024, https://www.consultant.ru/document/cons_doc_LAW_61798/

ISSN 2181-3187

3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ https://www.consultant.ru/document/cons_doc_LAW_61798/

4. Abdullayev, Shohzod. "KIBERJINOYATLARNI TERGOV QILISHDA XALQARO-HUQUQIY HAMKORLIK: MUAMMOLAR VA IMKONIYATLAR." Conferencea (2023): 38-49.