XXI ASR TALABI – KIBERXAVFSIZLIKNI TA'MINLASH

Iqboloy Ummatova

Toshkent davlat yuridik universiteti Xalqaro huquq va qiyosiy huquqshunoslik fakulteti 2-kurs talabasi

e-mail: iqboloyummatova27gmail.com.

Annotatsiya. *Mazkur maqola doirasida muallif tomonidan kiberxavfsizlik tushunchasi va uning mohiyati, kiberxavfsizlik bo'yicha mamlakatdagi qonunchilik hujjatlari yoritib berilgan. Shuningdek, kiberxavfsizlik holati statistik ma'lumotlar asosida tahlil qilingan hamda mamlakatdagi kiberjinoyatlar asosiy sabablari va ularning oldini olish choralari yoritilgan.*

Kalit so'zlar. *Kiber, kiberxavfsizlik, xakerlik hujumi, axborot-kommunikatsiya, kiberjinoyat, raqamli gigiyena.*

Аннотация. *В рамках данной статьи автором были освещены понятие и сущность кибербезопасности, законодательные акты страны по кибербезопасности. Также анализируется состояние кибербезопасности на основе статистических данных и освещаются основные причины киберпреступлений в стране и меры по их предотвращению.*

Ключевые слова. *Кибер, кибербезопасность, взлом, информационные коммуникации, киберпреступность, цифровая гигиена.*

Annotation. *Within the framework of this article, the author covered the concept of cyber security and its essence, legislative acts in the country on cyber security. In addition, the state of cyber security was analyzed based on statistics and covered the main causes of cybercrime in the country and measures to prevent them.*

Keywords. *Cybersecurity, hacking attack, Information Communication, cybercrime, digital hygiene.*

Axborotlashgan hozirgi zamonaviy dunyomizni turli xildagi gatjetlarsiz va internet aloqalarisiz tasavvur qilishimiz qiyin. Zamonaviy axborot texnalogiyalari, elektron xizmatlar hayotimiz ajralmas qismiga tobora aylanib bormoqda. Bularning barchasi insoniyat hayotini birmuncha osonlashtirayotgani rost. So‘nggi vaqtlarda “kiberxavfsizlik” tushunchasi juda ko‘p ishlatilmoqda. Ammo bu tushunchaning nimaligi haqida ko‘pchilik aholimizda aniq fikrlar mavjud emas. Birinchi navbatda mazkur tushunchani ta’riflab o‘tishimiz maqsadga muvofiq. **“Kiber”** atamasi odatda kompyuterlar, axborot texnologiyalari yoki internet bilan bog’liq narsalarni anglatadi. Buni yaxshiroq tushunish uchun uni kompyuterlar va internetga tegishli maxsus so’z sifatida tasavvur qilish maqsadga muvofiq. Xavfsizlik – bu xavf yoki tahdiddan xoli bo’lish va xavfsiz bo’lish holatini anglatadi. Shunday qilib, agar ikkita so’zni birlashtirsak, “kiberxavfsizlik” kompyuterlarni, tarmoqlarni va internetga ulangan har qanday qurilmani har qanday xavf yoki tahdiddan xavfsiz saqlashni anglatadi. Xususan, CSEC2017 Joint Task Force (CSEC2017 JTF) kibyerxavfsizlikka quyidagicha ta’rif bergan: **kiberxavfsizlik** – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. Bugungi kunda kiberxavfsizlikni ta’minlash xalqaro tusdagi asosiy vazifalardan biri hisoblannadi. Kiberxavfsizlikning ta’minlanmasligi katta hajmdagi axborotlarning xavf ostida qolishini ya’ni kiberjinoyat qurboniga aylanishini anglatadi. Shu o'rinda «Kiberjinoyatchilik» tushunchasiga kelsak, axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik, ma'lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o'g'irlash (fishing va farming) va boshqa turli huquqbuzarliklar bilan izohlanadi. Bugungi kunda

aholimiz orasida kiberxavfsizlik bo‘yicha huquqiy ongning yetarli darajada bo‘lmaganligi sababli kiberjinoyat qurbonlari ko‘paymoqda.

Normativ-huquqiy hujjatlar tahlili.

Mazkur munosabat yangi kirib kelganligi bois mamlakatimizda uni huquqiy jihatdan tartibga solish talab etildi. Shuning uchun 2022-yilda O‘zbekiston Respublikasining **„Kiberxavfsizlik to‘g‘risidagi”** qonuni qabul qilindi. Qonunga binoan, **Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi** deb belgilandi.[1] Mazkur qonunda binoan kiberxavfsizlikni ta’minlashdagi asosiy prinsiplar – qonuniylik, shaxs va davlat manfaatlarini himoya qilish, sohaga yagona yondashuv, tizimni yaratishda (davlat xaridlarida) mahalliy ishlab chiqaruvchilarga ustuvorlik berish, xalqaro hamkorlik uchun ochiqlik hisoblanadi.

Shuningdek, 22.09.2023 yilda O‘zbekiston Respublikasi Davlat xavfsizlik xizmati raisining “**O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risidagi nizomni tasdiqlash haqida**” buyrug‘i qabul qilindi. Mazkur hujjat O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibini belgiladi. Ushbu hujjatga muvofiq kiberxavfsizlik subyektlarining axborot tizimlari va resurslari hamda muhim axborot infratuzilmasi obyektlari toifasiga kiritilgan axborot tizimlarini, shuningdek texnik topshiriqlar loyihalarini kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish **“Kiberxavfsizlik markazi”** davlat unitar korxonasi tomonidan amalga oshirilishi belgilandi.

"Kiberxavfsizlik markazi" davlat unitar korxonasi nomi bilan 14.09.2019 yildagi PQ-4452-son O‘zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni

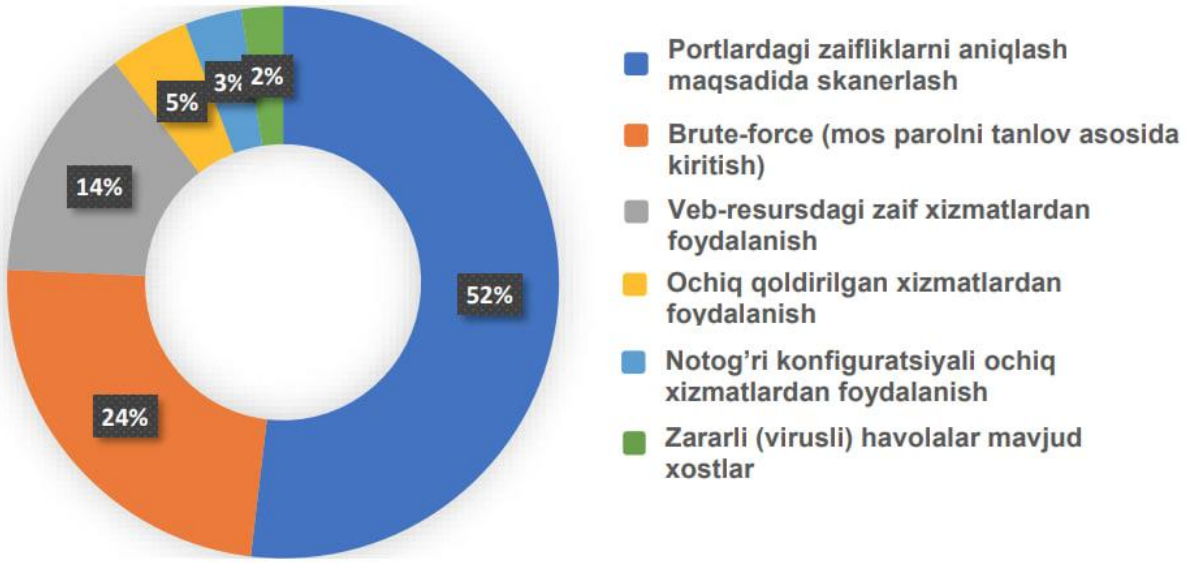
[1] O‘zbekiston Respublikasining ,,Kiberxavfsizlik to‘g‘risidagi” qonuni 2022

himoya qilish tizimini takomillashtirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida"gi qaroriga muvofiq faoliyat yuritib kelmoqda.

Statistik tahlil.

Ichki ishlar vazirligi 2022 yil boshida O‘zbekistonda **so‘nggi uch yilda kiberjinoyatlar 8,3 baravarga ko‘payib,** umumiy jinoyatchilikning qariyb 5 foiziga yetganini ma’lum qilgandi. Bu jinoyatlar qatorida noqonuniy bank-moliya operatsiyalari 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 sanalgan.

O‘zbekiston Kiberxavfsizlik markazining 2022 yildagi hisobotida aytilishicha , milliy kibermakonda zararli tarmoq faoliyati bilan bog‘liq **65 million** hodisa aniqlangan.[2] Ularni quyidagi kesimda turlarga ajratish mumkin;



[2] O‘zbekiston Kiberxavfsizlik markazining 2022 yil hisoboti

Kiberxavfsizlik markazi “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash” bo‘yicha 2022 yil uchun hisobotini e’lon qilingan. Unga muvofiq 2022-yil holatiga ko‘ra, O‘zbekiston Respublikasining internet tarmog’i “.UZ” segmentida 110 000 dan ortiq veb-sayt domenlari ulangan bo‘lib, shulardan 38 000 dan ortig‘i faol domenlardir. Ularning **14 000 dan ortig‘i xavfsiz** ya’ni SSL sertifikati bilan himoyalangan domenlar. Internet tarmog‘ining milliy segmentida joylashgan davlat va xo‘jalik boshqaruvi organlarining rasmiy veb-saytlarida 855 ta hodisa aniqlangan bo‘lib, buning natijasida davlat idoralarining veb-saytlari umumiy hisobda 1 570 659 daqiqa davomida ishdan chiqishiga olib kelgan. “.UZ” domen zonasidagi veb-saytlarning uzluksiz monitoringi davomida 236 ta kiberxavfsizlik insidenti aniqlanib, ularning asosiy qismi ruxsatsiz kontent yuklash (191 ta) hamda asosiy oynani ruxsatsiz o’zgartirish (19 ta) bilan bog’liq bo’lgan insidentlardir. Aniqlangan insidentlarning tahlili shuni ko’rsatmoqdaki, davlat idoralarining veb-saytlari (50 ta) xususiy sektor vakillarining veb-saytlaridan (186 ta) ko’ra, 3 barobar kamroq hujumlarga uchragan. Zararli kontentni aniqlash va uning axborot makonidagi huquqbuzarliklarga aloqadorligini tahlil qilish doirasida kiberxavfsizlik insidentlari tekshirilib, ularni amalga **oshirish sabablari va usullari** aniqlandi. “.UZ” domen zonasidagi veb-saytlarga muvaffaqiyatli hujumlarning asosiy sabablari quyidagilar:

- veb-saytlar ishlashida plaginlar va dasturiy ta'minot komponentlarining eskirgan versiyalari (CMS, mavzu shablonlari, kutubxonalar va boshqalar) dan foydalanish. Xususan, aksariyat hollarda pochta xizmatlari va masofaviy ulanish modullarida kritik darajadagi zaifliklar aniqlangan. **(34%);**
- veb-saytlar ishida qo'llanilmaydigan dasturiy vositalarning, shu jumladan, ishonchli bo’lmagan manbalardan yuklab olingan konfiguratsiya fayllarining ortiqchaligi **(8%);**
- parol siyosatiga amal qilinmaslik **(58%).** Xususan, tekshiruvlar natijasida axborot tizimlari va resurslari, shuningdek, ulardan foydalanuvchilarning

kiberxavfsizligiga tahdid solishi mumkin bo'lgan 179 ta zararli fayl va skriptlar aniqlangan.

Kiberjinoyatlar asosiy sabablari va ularning oldini olish choralari.

So'nggi yillarda O'zbekistonda kiberjinoyatlar soni bir necha baravarga oshib ketgan. Yurtimizda kiberjinoyatchilikning asosiy quyidagi turlari ko'p uchramoqda:

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

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

— ijtimoiy tarmoqda zo‘rlik ishlatish bilan qo‘rqitish, haqorat, suitsid holatlari (kiberbulling) va boshqalar.

Xorijiy davlatlar (Turkiya, Janubiy Koreya, Birlashgan Arab Amirliklari) tajribasi o‘rganilganda, aholida internetdan foydalanish madaniyatini shakllantirish orqali ularni ehtimoliy xavflardan barvaqt ogoxlantirish bu — internetdagi tahdidlarga qarshi kurashishdagi **eng samarali usuli** ekanligi ma’lum bo‘ldi. Shuning uchun barcha maqbul usullardan foydalanilgan holda (ommaviy axborot vositalari, targ‘ibot tadbirlari va boshqalar) aholimiz kiberjinoyatlar haqida ogohlantirilmoqda. Ammo shunga qaramasdan, aholimiz orasida kiberjinoyatlar qurbonlari soni yildan yilga oshmoqda. Masalan, birgina Toshkent shahrining o‘zida 2021-2023 yillar oralig‘ida kiberjinoyatlar soni **ikki barobarga oshgan**. TAD Industries texnik direktori Erkin Normatovga bayonotiga ko‘ra, kiberjinoyatlarning yarmidan ko‘pi **bank kartalaridan pul o‘g‘irlashga oid**.

Kiberxavfsizlikka erishish har bir inson o‘zining xavfsizlik choralarini ko‘rishidek bir qarashda oddiydek ko‘ringan, lekin, katta ahamiyatga ega bo‘lgan qadamlardan boshlanadi. Bu borada raqamli gigenaga amal qilish eng muhim qadamdir. **Raqamli gigiyena** – biz kundalik turmushimizni ularsiz tasavvur qilolmaydigan ijtimoiy tarmoqlar hamda elekton qurilmalar, shuningdek, internet jahon tarmog‘idan xavfsiz foydalanish tartib-qoidalaridir. Ilmiy tomondan qaralganda esa, “raqamli gigiena odamlarni kiberxatarlarni minimallashtirish maqsadida muntazam ravishda raqamli amaliyotlarni bajarishga undovchi vositadir.[3] Bundan tashqari yuqorida ta’kidlaganimiz bank kartadan pul o‘g‘irlash yoxud o‘zga kishining nomiga onlayn kredit olish kabi holatlardan aholimiz ogoh bo‘lishi lozim. Ya’ni turli yo‘llar orqali (masalan, o‘zini bank xodimiz sifatida tanishtirib telefon raqamga kelgan sms xabarnomani aytishini so‘rash) shaxsiy ma’lumotlar begona shaxslar tomonidan so‘ralganda uni oshkor qilmaslik darkor. Qachonki, har bir inson eng kamida o‘zining kiberxavfsizligini ta’minlashga intilsa bu ushbu shaxsning kiberjinoyat qurboni bo‘lishi mumkinligi ehtimolini anchagina kamaytiradi va buning natijasida respublika miqyosida kiberjinoyat qurbonlari soni birmuncha kamayishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasining ,,Kiberxavfsizlik to‘g‘risidagi” qonuni 2022
2. O‘zbekiston Kiberxavfsizlik markazining 2022 yil hisoboti
3. J.Zoilboyev ,, Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim” Maqola-2022

[3] J.Zoilboyev ,, Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim” Maqola-2022