IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 21 Issue 02 May 2026

KIBERJINOYATLAR VA ULARNING OLDINI OLISHNING HUQUQIY YECHIMLARI

Shomurodov Ulug‘bek
doi: https://doi.org/10.5281/zenodo.20390524

Annotatsiya: Ushbu maqolada kiberjinoyatlarning mazmun-mohiyati, ularning shaxs, jamiyat va davlat xavfsizligiga tahdidi hamda O‘zbekiston Respublikasida kiberjinoyatlarning oldini olishga qaratilgan huquqiy yechimlar tahlil qilinadi. Shuningdek, raqamli savodxonlikni oshirish, axborot xavfsizligini ta’minlash va fuqarolarning huquqiy madaniyatini yuksaltirish masalalariga alohida e’tibor qaratilgan. Maqolada amaldagi qonunchilik normalari va “Raqamli O‘zbekiston – 2030” strategiyasi doirasida amalga oshirilayotgan chora-tadbirlar yoritilgan.

Kalit so‘zlar: Kiberjinoyat, axborot xavfsizligi, huquqiy javobgarlik, raqamli savodxonlik, raqamli xavfsizlik, firibgarlik, axborot tizimlari, profilaktika.

Аннотация (на русском языке): В статье рассматривается сущность киберпреступлений, их влияние на безопасность личности, общества и государства, а также анализируются правовые решения, направленные на предотвращение киберпреступлений в Республике Узбекистан. Особое внимание уделено вопросам повышения цифровой грамотности, обеспечения информационной безопасности и повышения правовой культуры граждан.

Kirish

So‘nggi yillarda O‘zbekiston raqamli iqtisodiyot yo‘lidan izchil rivojlanmoqda. Elektron hukumat, onlayn to‘lovlar, masofaviy ta’lim va elektron savdo tizimlarining kengayishi fuqarolar hayotini sezilarli darajada yengillashtirdi.

Biroq raqamli texnologiyalar rivoji bilan birga kiberjinoyatlar deb ataluvchi yangi turdagi xavf-xatarlar ham yuzaga kelmoqda. Kiberjinoyatlar — bu zamonaviy jamiyat xavfsizligiga tahdid soluvchi, shaxsiy hayot, moliyaviy barqarorlik va davlat axborot tizimlariga zarar yetkazuvchi noqonuniy harakatlardir. Shu bois, ularning oldini olish va huquqiy jihatdan tartibga solish O‘zbekiston uchun dolzarb vazifadir.

Asosiy qism

1. Kiberjinoyat tushunchasi va turlari

Kiberjinoyat — bu kompyuter, internet yoki boshqa raqamli vositalardan foydalanib sodir etiladigan, shaxs, tashkilot yoki davlat manfaatlariga zarar yetkazuvchi harakatlardir.

Ularning asosiy turlari quyidagilardan iborat:

- bank kartalaridan noqonuniy foydalanish;
- shaxsiy ma’lumotlarni o‘g‘irlash;
- zararli dasturlar (viruslar) tarqatish;
- firibgarlik saytlarini yaratish;
- axborot tizimlariga ruxsatsiz kirish va kiberhujumlar uyushtirish.

2. Huquqiy asoslar va tarixiy nuqtai nazar

O‘zbekiston Respublikasining Birinchi Konstitutsiyasi 1992-yil 8-dekabrda qabul qilingan bo‘lib, unda inson huquqlari, shaxs daxlsizligi va davlat manfaatlarini himoya qilishga oid asosiy tamoyillar belgilangan. Mazkur konstitutsion asoslar hozirgi kunda ham raqamli xavfsizlik va axborot erkinligi sohasida huquqiy siyosatning poydevorini tashkil etadi.

Shuningdek, “Axborotlashtirish to‘g‘risida”gi (2003-yil, yangilangan tahrir – 2022-yil) va “Axborot xavfsizligi to‘g‘risida”gi Qonunlar bilan axborot tizimlarining daxlsizligi va ulardan qonuniy foydalanish kafolatlangan.

3. Huquqiy javobgarlik masalalari

O‘zbekiston Respublikasining Jinoyat kodeksida kiberjinoyatlar uchun aniq huquqiy javobgarlik belgilangan.

- 278^1-modda — “Axborot tizimlariga ruxsatsiz kirish” holatlari uchun javobgarlik;
- 141^1-modda — shaxsiy hayot daxlsizligini buzish;
- 141^2-modda. Shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilikni buzish
- 141^3-modda. Shaxsning sha’nini va qadr-qimmatini kamsituvchi hamda inson hayotining sir tutiladigan tomonlarini aks ettiruvchi ma’lumotlarni oshkor qilish
- 168-modda — firibgarlik, shu jumladan onlayn firibgarlik.

Mazkur moddalarga ko‘ra, axborot tizimlariga noqonuniy kirish, ularni ishdan chiqarish yoki ma’lumotlarni o‘zgartirish, zararli dasturlarni tarqatish, yoki tizimlarni falajlash (DDoS) kabi harakatlar uchun jarima, ma’muriy qamoq yoki ozodlikdan mahrum etish jazosi belgilanadi[1].

4. Kiberjinoyatlarning oldini olish choralari

So‘nggi yillarda O‘zbekistonda axborot xavfsizligi siyosati izchil kuchaytirildi. “Raqamli O‘zbekiston – 2030” strategiyasi doirasida davlat va xususiy sektorda kiberxavfsizlikni ta’minlash bo‘yicha qator tashkiliy va huquqiy chora-tadbirlar amalga oshirilmoqda.

Kiberxavfsizlik markazining rasmiy ma’lumotlariga ko‘ra, 2024-yilda 12 milliondan ortiq kiberhujum urinishlari qayd etilgan[2]. Bu 2023-yilga nisbatan 35 foizga ko‘pdir.

Fuqarolar uchun amaliy tavsiyalar:

- Shaxsiy ma’lumotlarni noma’lum saytlarga kiritmaslik;
- Parollarni muntazam yangilab turish;
- Shubhali havolalarni bosmaslik;
- Bank yoki davlat nomidan kelgan xabarlarning haqiqiyligini tekshirish.

5. Qo‘shimcha yechim va takliflar

1. Kiberjinoyatlarga ixtisoslashgan tergov va sud bo‘limlarini mustahkamlash. Bu dalillarni to‘plash, ekspertiza o‘tkazish va jinoyatchilarni tezda fosh etish imkonini beradi.

2. Fuqarolar uchun bepul “Kiberxavfsizlik markazlari” tashkil etish. Ular aholiga maslahatlar berib, kiberfiribgarlik qurbonlariga yuridik yordam ko‘rsatadi.

3. Raqamli savodxonlikni oshirish. Ta’lim muassasalari, OAV va jamoat tashkilotlari orqali tizimli targ‘ibot olib borish – profilaktikaning eng samarali usulidir.

Kiberjinoyatlarning oldini olish choralari

O‘zbekiston kiberxavfsizlik bo‘yicha hududda yetakchi davlatlardan biriga aylanish maqsadida bir qator islohotlarni amalga oshirmoqda.

Davlat darajasidagi chora-tadbirlar:

- **“Raqamli O‘zbekiston – 2030” strategiyasi** doirasida axborot tizimlarining himoya darajasi kuchaytirildi.
- **Kiberxavfsizlik markazi** tomonidan axborot tizimlari holati monitoring qilinmoqda.
- 2024-yilda **12 milliondan ortiq kiberhujum urinishlari** aniqlangan bo‘lib, bu kiberxavfsizlikning muhimligini yana bir bor tasdiqlaydi.

Tashkiliy choralar:

- davlat idoralarining axborot tizimlari muntazam auditdan o‘tkazilishi;
- davlat xizmatchilari uchun maxsus o‘quv dasturlari;
- bank va moliya sektorida PCI-DSS standartlarini joriy etish.

Aholi uchun profilaktik choralar:

- shubhali havolalardan foydalanmaslik;
- ikki bosqichli autentifikatsiyani yoqish;
- bank xabarlarining haqiqiyligini tekshirish;
- internetda shaxsiy ma’lumotlarni imkon qadar cheklash.

Xorijiy davlatlarning kiberxavfsizlik sohasidagi tajribasi va O‘zbekiston uchun mos yo‘nalishlar

Bugungi globallashuv sharoitida kiberjinoyatlarga qarshi kurash faqat milliy darajada emas, balki xalqaro hamkorlik vositasida samarali kechmoqda. Rivojlangan davlatlar bu borada aniq strategiyalar, kuchli huquqiy baza va zamonaviy texnologiyalar asosida ishlamoqda. Ularning tajribasini o‘rganish O‘zbekiston uchun ham dolzarb ahamiyatga ega.

1. AQSH tajribasi

AQSH kiberxavfsizlik bo‘yicha dunyodagi yetakchi davlatlardan biri bo‘lib, Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA) va Homeland Security kabi tuzilmalari orqali kiberhujumlarning oldini olish bo‘yicha keng ko‘lamli ishlar olib boradi. Muhim jihati — davlat va xususiy sektor o‘rtasida real vaqt rejimida ma’lumot almashish tizimi ishlab chiqilgan.
Shuningdek, "Cybersecurity Framework" (NIST) — butun dunyo bo‘yicha kiberxavfsizlik standartlarining asosiga aylangan.

2. Yevropa Ittifoqi (YI) tajribasi

Yevropa davlatlarida kiberxavfsizlik ENISA (European Union Agency for Cybersecurity) tomonidan muvofiqlashtiriladi. YIning eng muhim huquqiy hujjatlaridan biri — **GDPR** bo‘lib, u shaxsiy ma’lumotlarni himoya qilishda eng qat’iy talablarni belgilaydi. Bundan tashqari, NIS2 direktivasi tarmoqlar va axborot tizimlari xavfsizligini oshirishga qaratilgan.

3. Janubiy Koreya tajribasi

Janubiy Koreya kiberxavfsizlikni texnologik yondashuv bilan kuchaytirgan davlat. Ular maktabdan boshlab "Cyber Hygiene" — raqamli gigiyena bo‘yicha ta’lim beradi. Davlat KISA (Korea Internet & Security Agency) orqali yirik kiberhujumlarni markazlashtirilgan tarzda boshqaradi. AI texnologiyalari asosida erta ogohlantirish va tahlil tizimlari mavjud.

O‘zbekiston uchun ahamiyati: Ta’lim muassasalarida raqamli xavfsizlik bo‘yicha majburiy darslar joriy etish, AI asosida kiberhujumlarni aniqlash markazlarini yaratish.

4. Singapur tajribasi

Singapur "Smart Nation" strategiyasi doirasida eng ilg‘or raqamli xavfsizlik tizimini yaratgan. "Cyber Security Agency of Singapore" (CSA) mamlakat bo‘ylab yagona boshqaruv markazi sifatida faoliyat yuritadi. Ular davlat xizmatchilari uchun doimiy kiberxavfsizlik treninglarini majburiy qilgan.

O‘zbekiston uchun eng maqbul yo‘nalishlar va ularni qo‘llash bo‘yicha batafsil tushuntirilgan takliflar

1. Yevropa Ittifoqi tajribasini qo‘llash: Shaxsiy ma’lumotlarni himoya qilish tizimini kuchaytirish

Nega mos keladi?

O‘zbekiston raqamli xizmatlarni tez sur’atlarda kengaytirmoqda: elektron hukumat, onlayn to‘lovlar, mobil ilovalar, elektron tibbiyot kartalari. Bu jarayonda fuqarolarning shaxsiy ma’lumotlari juda katta hajmda to‘planadi. Yevropa Ittifoqidagi GDPR shaxsiy ma’lumotlarni eng yuqori darajada himoya qiluvchi qonun hisoblanadi.

O‘zbekistonda qanday qo‘llash mumkin?

- “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonunni GDPRga yaqinlashtirish:
ma’lumot egasidan rozilik olish, ma’lumotni o‘chirish huquqi (right to be forgotten), ma’lumotni minimal yig‘ish tamoyili.

- Ma’lumotlar ombori va serverlarni himoyalash bo‘yicha xalqaro standartlar (ISO/IEC 27001) joriy etish.

- Ma’lumotlar bilan ishlaydigan korxonalarni auditdan o‘tkazish.

Kutiladigan foyda:

- Onlayn xizmatlarga bo‘lgan ishonch oshadi,

- Kiberfiribgarlik va shaxsiy ma’lumotlar o‘g‘irlanishining oldi olinadi.

2. AQSH tajribasi: Davlat–xususiy sektor hamkorligini kuchaytirish

Nega mos keladi?

Kiberhujumlar ko‘proq banklar, mobil operatorlar, onlayn to‘lov tizimlari va xususiy IT-kompaniyalarni nishonga oladi. O‘zbekiston iqtisodiyotida ham bu yo‘nalish jadal rivojlanmoqda va xavfsizlik darajasi barcha uchun bir xil bo‘lishi zarur.

AQSHda CISA va xususiy kompaniyalar o‘rtasidagi ma’lumot almashish tizimi (threat-sharing) kiberhujumlarni erta aniqlashga yordam beradi.

O‘zbekistonda qanday qo‘llash mumkin?

- Yagona milliy “Cyber Threat Sharing Platform” yaratish.

Unda banklar, Uztelecom, UZINFOCOM, to‘lov tizimlari, xususiy IT-kompaniyalar o‘zaro real vaqt rejimida hujumlar haqida ma’lumot almashadi.

- Xususiy sektorni jalb qilgan holda milliy kiberxavfsizlik mashg‘ulotlari tashkil etish.
- Kiberhujumlarga qarshi tezkor javob beruvchi hamkor guruhlar (CERT) tashkil etish.

Kutiladigan foyda:

- Hujumlar dastlabki bosqichda aniqlanadi,
- Muammolarni har bir tashkilot alohida emas, balki umumiy tizim orqali hal qiladi.

3. Janubiy Koreya tajribasi: Ta’lim tizimida raqamli xavfsizlikni joriy etish

Nega mos keladi?

Bugun O‘zbekistonda internetdan eng ko‘p foydalanadigan qatlam — o‘quvchilar va talabalar. Kiberfiribgarlar aynan shu guruhni nishonga oladi (onlayn o‘yinlar, ijtimoiy tarmoqlar, mobil ilovalar orqali).

Janubiy Koreya tajribasida esa raqamli gigiyena maktablardan boshlab o‘rgatiladi.

O‘zbekistonda qanday qo‘llash mumkin?

- Maktab va kollejlar uchun “Raqamli xavfsizlik asoslari” fanini joriy etish.
- O‘quv dasturlarida quyidagi ko‘nikmalarni o‘rgatish:

— parol yaratish,
— shaxsiy ma’lumotni himoya qilish,
— internetda xavfsiz muomala.

- O‘qituvchilar uchun maxsus malaka oshirish dasturlari.

Kutiladigan foyda:

- Yoshlar kiberfiribgarlik qurboniga kamroq aylanadi,
- Uzun muddatda kiberxavfsizlik madaniyati shakllanadi.

4. Singapur modeli: Davlat xizmatchilari uchun kiberxavfsizlik sertifikatsiyasi

Nega mos keladi?

Davlat organlarining ko‘pi katta hajmda maxfiy axborot bilan ishlaydi. Inson omili sababli yuzaga keladigan xatoliklar (phishing linklarga kirish, zararli fayllarni yuklash, noto‘g‘ri parol siyosati) davlat tizimlariga jiddiy zarar yetkazishi mumkin.

Singapurda davlat xizmatchilari majburiy ravishda muntazam treninglardan o‘tadi.

O‘zbekistonda qanday qo‘llash mumkin?

- Barcha davlat xodimlari uchun majburiy yillik kiberxavfsizlik imtihoni joriy etish.
- Davlat organlarida axborot xavfsizligi bo‘yicha ichki bo‘limlar tashkil etish.

• Maxsus amaliy mashg‘ulotlar: phishing-testlar, zararli fayl simulyatorlari, kiberhujum ssenariylari.

Kutiladigan foyda:

• Davlat tizimlariga qarshi ichki xatoliklar keskin kamayadi,

• Axborot tizimlarining ishonchliligi oshadi.

5. Xalqaro hamkorlikni kengaytirish

Nega mos keladi?

Kiberjinoyatlar ko‘pincha transchegaraviy bo‘ladi — jinoyatchi boshqa davlatdan turib hujum uyushtirishi mumkin. Shuning uchun O‘zbekiston ham xalqaro tizimlarga qo‘shilishi zarur.

O‘zbekistonda qanday qo‘llash mumkin?

• INTERPOL Cybercrime departamenti bilan hamkorlikni mustahkamlash.

• ENISA, CISA bilan qo‘shma treninglar va seminarlar o‘tkazish.

• Qozog‘iston, Qirg‘iziston va boshqa qo‘shni davlatlar bilan Markaziy Osiyo kiberxavfsizlik alyansini yaratish.

Kutiladigan foyda:

• Transchegaraviy hujumlarni aniqlash osonlashadi,

• O‘zbekiston global kiberxavfsizlik tizimining faol ishtirokchisiga aylanadi.

Xulosa

Kiberjinoyatlar bugungi globallashuv davrida eng dolzarb huquqiy muammolardan biridir. Unga qarshi kurashda nafaqat davlat organlari, balki har bir fuqaroning ongli ishtiroki muhim ahamiyat kasb etadi. Huquqiy javobgarlikni kuchaytirish bilan bir qatorda, raqamli madaniyatni yuksaltirish va fuqarolarning huquqiy ongini oshirish zarur. Jinoyat huquqi bu borada adolat, xavfsizlik va qonun ustuvorligini ta’minlovchi mustahkam poydevor bo‘lib qoladi. Shuningdek, kiberxavfsizlikni ta’minlashda **xalqaro tajribalarni o‘rganish**, ilg‘or texnologiyalar va innovatsiyalarni joriy etish, hamda raqamli savodxonlikni kengaytirish muhim ahamiyatga ega. Fuqarolarning shaxsiy ma’lumotlarini himoya qilish, onlayn xavfsizlikka rioya qilish va jamoatchilik bilan hamkorlik qilish kiberjinoyatlarni oldini olishda samarali vositalardan biridir. Shu bilan birga, davlat va xususiy sektorning integratsiyalashgan chora-tadbirlari kiberxavfsizlik tizimini yanada mustahkamlashga xizmat qiladi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining Konstitutsiyasi. – Toshkent, 1992. (yangilangan tahrir – 2023-yil).
2. O‘zbekiston Respublikasi Jinoyat kodeksi. – Toshkent, 2023. Lex.uz
3. “Raqamli O‘zbekiston – 2030” strategiyasi. – Prezident.uz
4. “Axborot xavfsizligi to‘g‘risida”gi Qonun. – Qonun hujjatlari ma’lumotlari milliy bazasi, 2022. Lex.uz

5. Cybersecurity.uz – O‘zbekiston Kiberxavfsizlik markazining rasmiy portali, 2024-yilgi hisobot. Cybersecurity.uz
6. “O‘zbekistonda 2024-yilda 12 mln kiberhujum qayd etildi.” – Kun.uz, 2025-yil 3-fevral
7. Mamatqulov A. *Kiberjinoyatlar va ularning oldini olishning huquqiy asoslari.* – Toshkent: TMI nashriyoti, 2024.
8. **European Union Agency for Cybersecurity (ENISA)** — rasmiy sayt- https://www.enisa.europa.eu/about-enisa
9. **Cyber Security Agency of Singapore (CSA)** — rasmiy sayt- https://www.csa.gov.sg
10. **Cybersecurity and Infrastructure Security Agency (CISA, AQSH)** — rasmiy sayt va yangiliklar bo‘limi- https://www.cisa.gov