

KIBERJINOYATLAR TASNIFI VA ULARGA QARSHI KURASHISHNING HUQUQIY ASOSLARI.

O'ZBEKISTON RESPUBLIKASI IIV AKADEMIYASI KURSANTI

Butunboyev Bobosher Qahramon o'g'li

O'ZBEKISTON RESPUBLIKASI IIV AKADEMIYASI RAQAMLI TEXNOLOGIYALAR VA AXBOROT

XAVFSIZLIGI KAFEDRASI BOSHIG'I O'RINBOSARI

A.F. Isaqov

Kalit so'zlar: *kiberjinoyat, turlari, tasnifi, kiberxavfsizlik, xalqaro tajriba, oldini olish, qarshi kurash, sodir etish usullari, mexanizm, axborot xavfsizligi, huquqiy asos, tahlil, huquqiy asos.*

Annotatsiya: *Ushbu maqola kiberjinoyatlar tushunchasi va ularning tasnifi, turlari, sodir etilish usullari va mexanizmlari, O'zbekiston Respublikasi va qator xorijiy davlatlar hududlarida sodir etilayotgan kiberjinoyatlar turlari va oqibatlarini tahlil qilishga bag'ishlangan. Maqolada kiberjinoyatlarga oid zamonaviy tahdidlar turlari, ularning o'sish dinamikasi, milliy xavfsizlik va huquqiy tizimga ko'rsatayotgan ta'siri, mavjud yondashuvlarning samaradorligi xorijiy davlatlarda qo'llanilayotgan ilg'or mexanizmlar hamda milliy va xoriji huquqiy normalari qiyosiy yondashuv asosida tahlil qilingan. Xususan, O'zbekistonda 2025-yilda qabul qilingan PQ-153-sonli Prezident farmoni asosida shakllantirilgan yangi huquqiy mexanizmlar va ularning amaliy tatbiqi ko'rib chiqilgan. Shuningdek, rivojlangan mamlakatlarning kiberxavfsizlik sohasidagi qonunchiligi solishtirma tahlil o'tkazilgan. Maqola yakunida mavjud muammolar aniqlanib, ularni bartaraf etishga qaratilgan aniq taklif va tavsiyalar berilgan.*

Ключевые слова: *киберпреступность, виды, классификация, кибербезопасность, международный опыт, профилактика, противодействие, методы совершения, механизм, информационная безопасность, правовая основа, анализ, правовая основа.*

Аннотация: *Данная статья посвящена анализу понятия киберпреступлений и их классификации, видов, способов и механизмов совершения, видов и последствий киберпреступлений, совершаемых на территории Республики Узбекистан и ряда зарубежных государств. Данная статья посвящена анализу понятия киберпреступлений и их классификации, видов, способов и механизмов совершения, видов последствий киберпреступлений, совершаемых на территории Республики Узбекистан и ряда зарубежных . В статье проанализированы современные виды угроз киберпреступности, динамика их роста, влияние на национальную безопасность и правовую систему, эффективность существующих подходов на основе сравнительного подхода передовых механизмов, используемых в зарубежных странах, а также национальных и зарубежных правовых норм. В частности, были рассмотрены новые правовые механизмы и их практическое применение, сформированные в Узбекистане на*

основании указа президента № ПК-153, принятого в 2025 году. Также был проведен сравнительный анализ законодательства развитых стран в области кибербезопасности. В конце статьи выявляются существующие проблемы и даются конкретные предложения и рекомендации, направленные на их устранение.

Keywords: *cybercrime, types, classification, cybersecurity, international experience, prevention, fight against, methods of occurrence, mechanism, information security, legal framework, analysis, legal framewor*

Annotation: *This article is devoted to analyzing the concept of cybercriminals and their classification, types, methods and mechanisms of occurrence, types and consequences of cybercriminals occurring in the regions of the Republic of Uzbekistan and a number of foreign countries. his article is devoted to analyzing the concept of cybercriminals and their classification, types, methods and mechanisms of occurrence, types and consequences of cybercriminals occurring in the regions of the Republic of Uzbekistan and a number of foreign countries. The article analyzes the types of modern threats to cybercrime, their growth dynamics, their impact on national security and the legal system, the effectiveness of existing approaches on the basis of a comparative approach to advanced mechanisms used in foreign countries and national and foreign huqui norms. In particular, new legal mechanisms and their practical application are considered, formed on the basis of the Presidential Decree PQ-153 adopted in Uzbekistan in 2025. A comparative analysis of the legislation of developed countries in the field of cyber security was also carried out. At the end of the article, the existing problems were identified and specific proposals and recommendations were made aimed at eliminating them.*

KIRISH

XXI asrda axborot texnologiyalarining jadal sur'atlar bilan rivojlanishi insoniyat hayotining barcha sohalariga kirib bordi. Shu bilan birga, raqamli muhitda yangi turdagi jinoyatlar – kiberjinoyatlar paydo bo'ldi. Kiberjinoyatlar nafaqat alohida shaxslarga, balki butun jamiyat va davlat xavfsizligiga ham jiddiy tahdid solmoqda. Ularning xavfi shundaki, jinoyatchilar jismoniy chegaralardan mustaqil ravishda, dunyoning istalgan nuqtasidan turib, axborot tizimlariga zarar yetkazish imkoniyatiga ega. Shu sababli kiberjinoyatlarga qarshi kurashish bugungi kunda har bir mamlakatning milliy xavfsizlik siyosatining ajralmas qismi bo'lib bormoqda.

Asosiy qism

Kiberjinoyatlar tushunchasi va mohiyati

Kiberjinoyat tushunchasi xalqaro miqyosda bir xil talqin qilinmasa-da, umumiy jihatdan u “kompyuter tarmoqlari, axborot tizimlari yoki raqamli qurilmalardan foydalangan holda amalga oshiriladigan noqonuniy harakatlar” sifatida e'tirof etiladi.

BMT va Interpol hujjatlarida kiberjinoyatlar — bu axborot resurslariga ruxsatsiz kirish,

ularni o'zgartirish, yo'q qilish yoki ulardan noqonuniy foydalanish bilan bog'liq jinoyatlar deb belgilanadi.

Kiberjinoyatlar nafaqat texnik vositalar orqali, balki ijtimoiy muhitdagi firibgarlik, psixologik manipulyatsiya (phishing, social engineering) kabi usullar bilan ham sodir etiladi.

Kiberjinoyatlarning tasnifi

Kiberjinoyatlar bir necha mezonlarga ko'ra tasniflanadi. Eng keng tarqalgan tasnif obyekti va maqsadiga ko'ra quyidagicha:

1. Axborot resurslariga qarshi jinoyatlar: ruxsatsiz kirish, viruslar yaratish va tarqatish, ma'lumotlarni o'chirish yoki o'zgartirish.

2. Moliyaviy sohadagi kiberjinoyatlar: onlayn banking tizimlariga hujumlar, plastik kartalar orqali firibgarlik, kriptovalyuta o'g'riligi.

3. Shaxsiy daxlsizlikka qarshi kiberjinoyatlar: shaxsiy ma'lumotlarni noqonuniy tarqatish, kiberbulling, onlayn tahdid va shantaj.

4. Davlat xavfsizligiga qarshi jinoyatlar: kiberjosuslik, dezinformatsiya, davlat axborot tizimlariga hujumlar, strategik tarmoqlarga zarar yetkazish.

O'zbekiston Respublikasida kiberjinoyatlarga qarshi kurashishning huquqiy asoslari O'zbekiston Respublikasi kiberjinoyatlarga qarshi kurashish sohasida mustahkam normativ-huquqiy bazaga ega.

Asosiy hujjatlar quyidagilardir:

–O'zbekiston Respublikasi Jinoyat kodeksi (278¹–278³-moddalar): kompyuter axborotiga ruxsatsiz kirish, tarmoqlarni buzish va axborot xavfsizligi qoidalarini buzish uchun javobgarlikni belgilaydi;

–“Axborotlashtirish to'g'risida”gi Qonun (2003, yangi tahrir 2021): axborot tizimlaridan qonuniy foydalanish tartibini belgilaydi;

–“Axborot xavfsizligi to'g'risida”gi Qonun (2019): axborot xavfsizligini ta'minlashning tashkiliy-huquqiy asoslarini belgilaydi;

–Prezident farmon va qarorlari: PF-3837-son (2018-yil) “Kiberxavfsizlikni ta'minlash tizimini takomillashtirish chora-tadbirlari to'g'risida”, PQ-357 (2022-yil) “Kiberxavfsizlik markazini tashkil etish to'g'risida”.

Mazkur hujjatlar asosida Axborot texnologiyalari vazirligi, Ichki ishlar vazirligi, Davlat xavfsizlik xizmati va Milliy gvardiya o'zaro hamkorlikda kiberjinoyatlarga qarshi faoliyat olib boradi.

Xalqaro huquqiy mexanizmlar va tajriba

Kiberjinoyatlar global muammo bo'lgani sababli, unga qarshi kurashda xalqaro hamkorlik muhim ahamiyat kasb etadi.

Asosiy xalqaro hujjatlar:

–Budapesht konvensiyasi (2001) – kiberjinoyatlarga qarshi birinchi xalqaro konvensiya bo'lib, 60 dan ortiq davlat tomonidan ratifikatsiya qilingan;

–Interpolning Milliy Kiberjinoyatlarga qarshi strategiyasi (National Cybercrime Strategy)

–

davlatlar o'rtasida axborot almashinuv tizimini kuchaytirish va tezkor javob mexanizmlarini joriy etishga qaratilgan;

–BMTning Kiberxavfsizlik rezolyutsiyalari (2020–2023) – xalqaro axborot makonida tinchlik va barqarorlikni ta'minlashni nazarda tutadi.

Ko'plab rivojlangan davlatlarda, xususan AQSh, Buyuk Britaniya, Janubiy Koreya va Singapurda kiberxavfsizlik agentliklari milliy mudofaa tizimining muhim bo'g'iniga aylangan.

Kiberxavfsizlik siyosati va amaliy mexanizmlar

Kiberjinoyatlarga qarshi samarali kurashish uchun nafaqat qonunchilik, balki amaliy mexanizmlar ham muhimdir.

Ular quyidagilardan iborat:

1. Huquqiy mexanizmlar – qonunlarni yangilash, xalqaro konvensiyalarni ratifikatsiya qilish.

2. Tashkiliy mexanizmlar – milliy CERT markazlari, tezkor javob guruhlarini tashkil etish.

3. Texnik mexanizmlar – antivirus tizimlari, xavfsizlik devorlari, DLP tizimlari.

4. Ta'limiy va ma'rifiy mexanizmlar – aholi va xodimlarning kiberxavfsizlik savodxonligini oshirish.

O'zbekiston Respublikasida "Cyber Security Center" faoliyati shu yo'nalishda muhim amaliy o'rin tutadi.

Tahlil va muammolar

Tahlillar shuni ko'rsatadiki, kiberjinoyatlarning soni har yili ortib bormoqda. Asosiy muammolar quyidagilardan iborat:

–texnologik vositalarning tez eskirishi;

–xalqaro hamkorlikdagi huquqiy tafovutlar;

–malakali kadrlar yetishmasligi;

–fuqarolarning raqamli madaniyat darajasining pastligi.

Shuningdek, jinoyatlarni isbotlash, dalillarni yig'ish va sudgacha bo'lgan tergov jarayonida texnik ekspertiza murakkabligi ham muhim to'siq hisoblanadi.

Taklif va tavsiyalar

1. Jinoyat kodeksiga yangi modda kiritish orqali kiberjinoyatlarning aniq turlarini huquqiy tasniflash.

2. Axborot xavfsizligi sohasida mutaxassislar tayyorlovchi oliy ta'lim muassasalarining o'quv rejasini xalqaro standartlarga moslashtirish.

3. Har bir davlat organida ichki kiberxavfsizlik bo'limlarini joriy etish.

4. Xalqaro tashkilotlar bilan (Interpol, Europol, ITU) hamkorlikni kengaytirish.

5. Raqamli madaniyatni oshirish bo'yicha ijtimoiy aksiyalar va o'quv dasturlarini yo'lga qo'yish.

XULOSA

Xulosa qilib aytganda, kiberjinoyatlar zamonaviy xavfsizlik muhitining eng dolzarb muammolaridan biridir. O'zbekiston Respublikasida ushbu sohada huquqiy asoslar shakllantirilgan bo'lsa-da, xalqaro tajriba asosida ularni yanada takomillashtirish zarur.

Kiberxavfsizlikni ta'minlash faqat hukumat yoki maxsus xizmatlarning vazifasi emas — bu butun jamiyatning, har bir fuqaroning umumiy mas'uliyatidir. Kelajakda raqamli sohada barqarorlikni ta'minlash uchun huquqiy, texnik va ma'rifiy chora-tadbirlar uyg'un holda olib borilishi lozim.

FOYDALANILGAN ADABIYOTLAR:

1. O'zbekiston Respublikasi Jinoyat kodeksi.
2. "Axborotlashtirish to'g'risida"gi Qonun (2003, 2021).
3. "Axborot xavfsizligi to'g'risida"gi Qonun (2019).
4. PF-3837-son Farmon, 2018-yil.
5. Interpol. National Cybercrime Strategy, 2022.
6. Budapest Convention on Cybercrime, 2001.
7. BMT rezolyutsiyalari, 2020–2023.
8. OECD. Cybersecurity Policy Framework, 2021.
9. ITU Global Cybersecurity Index, 2022.