

KIBERJINOYATLAR VA ULARNING HUQUQIY JIHATLARI.

Xursanboyev Javohir Baxtiyor o'g'li

Rustamov Farrux Amirovich

Maxmudov Sherzod Erkinovich

Imamaliyev Aybek Turapbayevich

Muhammad Al-Xorazmiy nomidagi Toshkent Axborot

Texnologiyalari Universiteti

Annotatsiya: Mazkur maqolada kiberjinoyatlar tushunchasi, ularning turlari, global va milliy miqyosda tarqalishi, shuningdek, huquqiy jihatdan tartibga solish masalalari tahlil qilinadi. O'zbekiston Respublikasi qonunchiligi, xalqaro tajriba hamda zamonaviy texnologik tahdidlar kontekstida kiberjinoyatlarning oldini olish yo'llari ko'rib chiqiladi. Maqolada statistik ma'lumotlar, huquqiy tahlillar va ekspertlar fikrlariga asoslangan ilmiy yondashuvdan foydalaniladi.

Kalit so'zlar: Kiberjinoyat, axborot xavfsizligi, kiberxavfsizlik, huquqiy tartibga solish, raqamli jinoyatlar, xalqaro huquq.

Axborot-kommunikatsiya texnologiyalarining rivojlanishi bilan birga, jamiyat yangi xavf-xatarlar bilan yuzma-yuz kelyapti. Jumladan, kiberjinoyatlar — kompyuter texnologiyalaridan foydalanib sodir etiladigan jinoyatlar — zamonaviy jamiyat uchun jiddiy muammoga aylangan. Bu turdagi jinoyatlar nafaqat shaxsiy manfaatlarga, balki davlat xavfsizligiga ham tahdid solmoqda. Shu bois, kiberjinoyatlarga qarshi kurashish masalasi huquqiy jihatdan dolzarb bo'lib bormoqda.

Kiberjinoyatlar axborot texnologiyalaridan foydalangan holda sodir etiladigan huquqbuzarliklar bo'lib, ular kompyuter tizimlari, tarmoqlari yoki raqamli qurilmalar orqali amalga oshiriladi. Ushbu jinoyatlar jamiyat, iqtisodiyot, shaxsiy hayot va davlat xavfsizligiga jiddiy tahdid soladi.





Kiberjinoyatlarning turlari

Kiberjinoyatlar quyidagi asosiy turlarga bo'linadi:

- Xakerlik (Hacking) – kompyuter tizimlariga ruxsatsiz kirish;
- Phishing – yolg'on e-mail yoki saytlar orqali foydalanuvchilarning shaxsiy ma'lumotlarini qo'lga kiritish;
- DDoS hujumlar – tarmoqlarni ishdan chiqarish maqsadida katta hajmdagi so'rovlar yuborish;
- Zararli dasturlar (malware, virus, trojanlar) – tizimlarga zarar yetkazish yoki ma'lumotlarni o'g'irlash;
- Moliyaviy firibgarlik – onlayn banking, elektron to'lov tizimlari orqali pul o'g'irlash;
- Kiberterrorizm – davlat yoki jamoat tuzilmalariga qarshi texnologik vositalar orqali hujum qilish;
- Shaxsiy hayotga tajovuz – ruxsatsiz videokuzatuv, shaxsiy ma'lumotlarni tarqatish.

Kiberjinoyatlarning xavfi

- Ma'lumotlarning yo'qotilishi yoki o'g'irlanishi;
 - Shaxsiy va tijorat sirlarining fosh bo'lishi;
 - Moliyaviy zarar;
 - Davlat organlari va muassasalarining ishi buzilishi;
 - Jamiyatda ishonchsizlik va xavotir kuchayishi.
- Kiberjinoyatlarga qarshi kurashish vositalari
- Kuchli parollar, antivirus dasturlari, xavfsiz tarmoqlar;
 - Axborot xavfsizligi bo'yicha ta'lim va ogohlikni oshirish;
 - Tizimlarni doimiy monitoring qilish;
 - Qonunchilikni takomillashtirish;
 - Huquq-tartibot organlarining malakasini oshirish.

Kiberjinoyatlarning huquqiy jihatlari

O'zbekiston qonunchiligida:



- Jinoyat kodeksining 278-prim va 278-1-moddalarida axborot texnologiyalari sohasidagi jinoyatlar belgilangan.

- Ma'muriy javobgarlik to'g'risidagi kodeksda esa ayrim kiberjinoyatlar uchun ma'muriy choralar ko'zda tutilgan.

- "Axborotlashtirish to'g'risida"gi Qonun, "Shaxsiy ma'lumotlar to'g'risida"gi Qonunlar axborot xavfsizligini huquqiy asosda mustahkamlab beradi.

Xalqaro huquqiy me'yorlar:

- Budapesht Konvensiyasi (2001) – kiberjinoyatlarga qarshi kurashish bo'yicha asosiy xalqaro hujjat;

- Interpol va Europol tomonidan tashkil etilgan kiberjinoyatga qarshi kurashish bo'linmalari;

- Davlatlararo axborot almashuvi va hamkorlik mexanizmlari.

O'zbekiston kiberjinoyatlarga qarshi kurashishda bir qator yutuqlarga erishgan bo'lsa-da, huquqiy bo'shliqlar mavjud. Masalan, barcha internet jinoyatlari Jinoyat kodeksida alohida modda bilan ko'rsatilmagan. Yangi texnologiyalar ortidan paydo bo'layotgan tahdidlar, jumladan, sun'iy intellekt va IoT qurilmalaridagi xavfsizlik masalalari hali yetarlicha tartibga solinmagan. Bu esa jinoyatchilar uchun huquqiy "bo'shliqlar"dan foydalanish imkonini yaratadi.

Xulosa

Kiberjinoyatlar zamonaviy dunyoda eng jiddiy tahdidlar qatoriga kiradi. Ularni aniqlash, oldini olish va jazolash uchun davlatlar zamonaviy texnologiyalardan foydalanish, qonunchilikni takomillashtirish va xalqaro hamkorlikni mustahkamlashi zarur.

Kiberjinoyatlar – zamonaviy davrning eng xavfli jinoyat turlaridan biri bo'lib, ularni huquqiy jihatdan tartibga solish doimiy yangilanishni talab qiladi.

Jinoyat kodeksiga kiberjinoyatlar bo'yicha alohida bob kiritish;

Raqamli xavfsizlik bo'yicha milliy strategiyani ishlab chiqish;

Sud va tergov organlarini kiberjinoyatlar bo'yicha maxsus o'quv dasturlarida tayyorlash;

Internetda faoliyat yurituvchi platformalarning huquqiy javobgarligini belgilovchi qonunlar qabul qilish.

Adabiyotlar.

1. Maillart, J.B. The limits of subjective territorial jurisdiction in the context of cybercrime. ERA Forum, 19, 2019, pp. 375–390. <https://doi.org/10.1007/s12027-018-0527-2>
2. Brenner, S.W. Toward a criminal law for cyberspace: distributed security. Journal of Technology Law and Policy, Vol.V (1). 2004
3. Renu & Pawan. Impact of Cyber Crime: Issues and Challenges. International Journal of Trend in Scientific Research and Development, Vol. 3, Issue 3, 2019, pp.1569-1572, <https://www.ijtsrd.com/papers/ijtsrd23456.pdf>
4. Iqbal F., Debbabi M., Fung B.C.M. Cybersecurity And Cybercrime Investigation. In: Machine Learning for Authorship Attribution and Cyber Forensics. International Series on Computer Entertainment and Media E-ISSN: 2224-3496
5. Statista. Cyber Crime & Security. Statistics and Market Data on Cyber Crime & Security, 2020, <https://www.statista.com/markets/424/topic/1065/cyber-crime-security>
6. Antonescu M. Birăub R. Financial and Non financial Implications of Cybercrimes in Emerging Countries, Procedia Economics and Finance. Vol. 32, 2015, pp. 618-621, [https://doi.org/10.1016/S2212-5671\(15\)014409](https://doi.org/10.1016/S2212-5671(15)014409)
7. Mulligan, D., Levi, M. Prevalence of Cyber Crime and its Effect on Economy, Idosr Journal of Arts and Management, 5(1), 2020, pp. 64-69
8. Understanding the costs of cyber crime. A report of key findings from the Costs of Cyber Crime Working Group, 2018, <https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime>

