

**KIBERJINOYATCHILIK- GLOBAL XAVF: DUNYO
QONUNCHILIGI SHARHI**

Umirzoqov Shoxrux Shovqiddin o'g'li

Toshkent davlat yuridik universiteti

Xalqaro huquq va qiyosiy huquqshunoslik fakulteti 1-kurs talabasi

E-mail: shoxruxumirzoqov07@gmail.com

Annotatsiya. Bilamizki, bugungi shiddat bilan rivojlanib borayotgan zamonaviy dunyoda texnologiyalar yildan yilga yangi bosqichga chiqqani sari kiberjinoyatchilik tushunchasi ham ommalashib bormoqda. Kiberjinoyatchilik iqtisodiyot, milliy xavfsizlik va shaxsiy hayotga tahdid soluvchi global muammo sifatida namoyon bo'lmoqda. Ushbu sharhda xalqaro va milliy qonunchilikda kiberjinoyatchilikka qarshi kurashishda qanday amaliyotlar va mexanizmlar qo'llanilishi va samaradorligi tahlil etiladi. Ushbu qisqa maqolada, BMT, Yevropa Kengashi va boshqa xalqaro tashkilotlarning konvensiyalari, shuningdek, AQSH, Yevropa va Osiyo mamlakatlarining milliy qonunchiliklarini ko'rib chiqamiz. Tadqiqotda qiyosiy huquqiy usulni qo'llagan holda, yuqorida sanalgan xalqaro huquq subyektlarining milliy qonunchiliklarini samaradorligi, hamkorlikdagi muammolar va raqamlik huquqlar himoyasi borasidagi masalalar muhokama qilinadi. Natijada qonunchilikdagi bir qancha bo'shliqlar bartaraf etish maqsadida kiberjinoyatchilikka qarshi kurashish bo'yicha yangi xalqaro shartnomalar tuzilishi kerakligi ta'kidlanadi.

Kalit so'zlar: kiberjinoyatchilik ,global tahdid, xalqaro qonunchilik, jinoyatchilik, raqamli huquqlar, qonunchilik sharhi.

Kirish

Zamonaviy axborot jamiyatda kiberjinoyatchilik nafaqat texnologik, balki ijtimoiy-iqtisodiy va siyosiy tahdid sifatida ommalashib bormoqda. Xarajatlar bo'yicha turlicha baholar mavjud bo'lishiga qaramay, sanoat hisobotlari shuni

ko'rsatadiki, kredit karta o'g'irligi, "ransomware" hujumlari va yirik korxonalarda, shuningdek, kichik va o'rta bizneslarda sodir bo'layotgan xavfsizlik buzilishlari kabi turli sohalarda global xarajatlar muntazam ravishda ortib bormoqda. Soha prognozlariga ko'ra, yaqin yillarda kriptojinoyatlar va "ransomware" hujumlari eng tez o'sayotgan kiberhujum turlari bo'lib qoladi, ularning dunyo miqyosidagi umumiy xarajatlari mos ravishda 2025-yilda yiliga 30 milliard AQSh dollariga, 2031-yilda esa 265 milliard AQSh dollariga yetishi kutilmoqda. Shuningdek, ma'lumotlar sizib chiqishi(data breach) holatlari ham yanada katta xarajatlarga sabab bo'lishi va har bir hodisa uchun rekord darajadagi – 4.35 million AQSh dollarlariga yetishi kutilgan [1]. Bu hodisa hamkorlikni yo'lga qo'yish zarurligini ta'kidlaydi, ya'ni global yondashuvni talab qiladi.

Kiberjinoyatlar to'g'risidagi konvensiya (shuningdek, Kiberjinoyatlar to'g'risidagi Budapesht konvensiyasi yoki Budapesht konvensiyasi sifatida ham tanilgan) milliy qonunlarni uyg'unlashtirish, tergov usullarini takomillashtirish va davlatlar o'rtasidagi hamkorlikni oshirish orqali Internet va kompyuter jinoyatlarini (kiber jinoyatlar) hal qilishga qaratilgan birinchi xalqaro shartnomadir. U Fransiyaning Strasburg shahrida Yevropa Kengashi tomonidan Yevropa Kengashining kuzatuvchi bir qancha davlatlari Kanada, Yaponiya, Filippin, Janubiy Afrika va AQShning faol ishtirokida ishlab chiqilgan. Ammo, uning cheklangan qamrovi va ba'zi davlatlarning ratifikatsiya qilmasligi muammolarni keltirib chiqarmoqda [2]. Masalan, Braziliya va Hindiston bu konvensiyani qabul qilmagan. 2020-yil dekabr holatiga ko'ra, 65 davlat konvensiyani ratifikatsiya qilgan, yana to'rtta davlat konvensiyani imzolagan, ammo uni ratifikatsiya qilmagan. Markaziy Osiyo, jumladan O'zbekistonda kiberjinoyatchilikka qarshi kurashish bo'yicha qonunchiliklari rivojlangan bo'lsa-

da, global standartlarga mos kelish masalasi hali ham dolzarb masala bo'lib qolmoqda [3].

Huquq nazariyasining vakillari, masalan A.Bendovschi ta'kidlashicha texnologiya ijtimoiy tarmoqlar, onlayn tranzaksiyalar, bulutli hisoblash va avtomatlashtirilgan jarayonlar bilan boshqariladigan dunyoda tez sur'atlarda rivojlanmoqda. Biroq, texnologiyaning rivojlanishi bilan bir qatorda kiberjinoyatchilik ham taraqqiy etmoqda — u doimo yangi hujum turlari, vositalar va usullarni ishlab chiqadi, bu esa hujumchilarga yanada murakkab yoki yaxshi nazorat qilinadigan muhitlarga kirib borish, ko'proq zarar yetkazish va hatto aniqlanmaslik imkonini beradi [4]. Ushbu sharhda qonunchilikning evolutsiyasi, samaradorligi va istiqbollari muhokama qilinadi.

Material va metodlar

Kiberjinoyatga qarshi kurashish, birgalikda hamkorlik faoliyatini olib borish, global yondashgan holda dunyo standartlariga mos qonunchiliklar qabul qilish uchun bizdan ko'p qirrali yondashuvni talab qiladi. Tadqiqotda tahlil va sintez, mantiqiy, tizimli, shuningdek, qiyosiy-huquqiy va rasmiy-huquqiy usullar qo'llanilgan. Manbalar sifatida BMT, Yevropa Kengashi va Jahon banki hisobotlari, milliy qonunlar va ilmiy adabiyotlar (ResearchGate, Google scholar) tanlangan. Tadqiqot davri – 2001–2025-yillar, global qamrovni o'z ichiga olgan.

Tadqiqot natijalari

Dunyo qonunchiligida kiberjinoyatchilikka qarshi kurashning asosiy ramkalari quyidagilardan iborat:

– Xalqaro daraja: Budapest konventsiyasi (68 davlat ratifikatsiya qilgan) kompyuter jinoyatlari, ma'lumot o'g'irlash va DDoS hujumlarini kriminalizatsiya

qiladi [5]. 2024-yilda BMT tomonidan qabul qilingan Kiberjinoyatchilikka qarshi konventsiya transmilliy hamkorlikni kuchaytirishga qaratilgan [6].

– Mintaqaviy daraja: Yevropa Ittifoqida GDPR (2018) va NIS2 (2022) shaxsiy ma'lumotlarni himoya qilish va infratuzilmani mustahkamlashni ta'minlaydi [7]. Osiyo-Pacifik mintaqasida ASEAN kiberxavfsizlik frameworki (2018) hamkorlikni belgilaydi [8].

– Milliy daraja: AQShda Computer Fraud and Abuse Act (CFAA, 1986, yangilangan 2023) hujumlarni jazoga tortadi, jazo muddati 10–20 yil [9]. Rossiyada “Axborot texnologiyalari va axborot himoyasi” to‘g‘risidagi federal qonun (2021) kiberterrorizmni taqiqlaydi [10]. O‘zbekistonda Kiberxavfsizlik to‘g‘risidagi qonun (2022) milliy tarmoqni himoya qilish mexanizmlarini belgilaydi [11].

Statistikaga ko‘ra, 2024-yilda 75% davlatlarda kiberjinoyatchilik qonunlari mavjud, ammo faqat 52% da elektron dalillarni yig‘ish protseduralari ishlab chiqilgan [12].

Tadqiqot natijalari tahlili

Tahlil shuni ko‘rsatadiki, global qonunchilikdagi muammolar yaqqol namoyon bo‘lmoqda. Masalan, Budapest kontvensiyasida Yevropa mamlakatlarida anchagina samarali bo‘lishiga qaramay, Osiyo va Afrika mamlakatlarida ratifikatsiya darajalari past. Bu holat kiberjinoyatchilikka qarshi kurashishda xalqaro hamkorlikni qurishda asosiy to‘siqlardan biridir.

Milliy qonunchilikni O‘zbekiston misolida ko‘radigan bo‘lsak, milliy qonun xalqaro standartlarga nisbatan mos keladi. Lekin, mutaxassis kabi resurslarning yetishmasligi amalga oshirishni sussaytiradi. Raqamli huquqlar va kiberjinoyatlarga qarshi kurashish bo‘yicha yangi qonunchilikni ishlab chiqishni

talab qiladi. Bundan tashqari O'zbekiston qonunchiligini boshqa davlatlar qonunchiligi bilan qiyosiy tahlil qilinganda ham o'ziga xos tuzatishlar kiritish imkoniyatini tug'diradi.

Xulosalar

Kiberjinoyatchili global tahdid sifatida qonunchilikda yangilanishlarni talab qiladi. Budapest va boshqa xalqaro kontvensiyalari qabul qilingan bo'lsa-da, ularning cheklanganligi va ko'plab davlatlarning ratifikatsiya qilmaganligi yangi xalqaro shartnomalar qabul qilinishi zarurligini ko'rsatadi. O'zbekiston qonunchiligi uchun Yevropa va AQSh tajribasini o'rganish va resurslarni ta'minlash tavsiya etiladi.

REFERENCES

1. World Bank. A Review of the Economic Costs of Cyber Incidents.
2. Council of Europe. Budapest Convention on Cybercrime. Strasbourg, 2001. Available at: <https://www.coe.int/en/web/conventions/full-list>.
3. UNCTAD. Cybercrime Legislation Worldwide. Geneva: UNCTAD, 2023, pp. 12–18.
4. Andreea Bendovschi Cyber-attacks-trends, patterns and security countermeasures.
5. Council of Europe. The Global State of Cybercrime Legislation 2013–2024. Strasbourg, 2024.
6. United Nations. Convention against Cybercrime. New York, 2024.
7. European Union. NIS2 Directive. Brussels, 2022.
8. ASEAN. Cybersecurity Framework. Jakarta, 2018.

-
9. U.S. Congress. Computer Fraud and Abuse Act (amended 2023).
Washington, DC.
 10. Russian Federation. Federal Law on Information Security (2021).
Moscow.
 11. Republic of Uzbekistan. Law on Cybersecurity (2022). Tashkent.
 12. ITU. Global Cybersecurity Index 2024. Geneva: ITU, 2024, p. 67.