KIBERJINOYATLARNING KLASSIFIKATSIYASI VA ZAMONAVIY TENDENSIYALARI

Komilov Diyorbek Zokir o‘g‘li
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi “Kiberxavfsizlikni huquqiy ta’minlash” yo‘nalishi magistratura bosqichi tinglovchisi
E-mail: diyorbekkomilov2404@gmail.com

ANNOTATSIYA
Mazkur maqolada kiberjinoyatlarning tavsiflanishi hamda ularning zamonaviy tendensiyalari tahlil qilinadi. Xususan, kiberjinoyatlarning asosiy klassifikatsiyasi, ularning amaliy ko‘rinishlari va so‘nggi yillarda kuzatilayotgan transformatsiya jaryonlari o‘rganiladi. Tadqiqot natijasida kiberjinoyatlarning murakkablashuvi, avtomatlashtirilishi va transmilliy xarakterining kuchayib borayotgani asoslab beriladi.

Kalit so‘zlar: kiberjinoyat turlari, axborot texnologiyalariga qarshi qaratilgan kiberjinoyatlar, axborot texnologiyalari vositasida sodir etiladigan kiberjinoyatlar, phishing, malware, ransomware, kiberjinoyatlar ximzat sifatida, kiberxavfsizlik, raqamlashtirish, sun’iy intellekt.

ABSTRACT
This article analyzes the characterization of cybercrimes and their modern trends. In particular, the main classification of cybercrimes, their practical manifestations, and the transformation processes observed in recent years are examined. As a result of the study, it is substantiated that cybercrimes are becoming increasingly complex, automated, and transnational in nature.

Keywords: types of cybercrime, cybercrimes against information technologies, cybercrimes committed using information technologies, phishing, malware, ransomware, cybercrime as a service, cybersecurity, digitalization, artificial intelligence.

АННОТАЦИЯ
В данной статье анализируются характеристика киберпреступлений и их современные тенденции. В частности, рассматриваются основная классификация киберпреступлений, их практические проявления, а также процессы трансформации, наблюдаемые в последние годы. В результате исследования обосновывается, что киберпреступления становятся всё более сложными, автоматизированными и приобретают транснациональный характер.

Ключевые слова: виды киберпреступлений, киберпреступления против информационных технологий, киберпреступления, совершаемые с использованием информационных технологий, фишинг, вредоносное программное обеспечение, программы-вымогатели, киберпреступность как услуга, кибербезопасность, цифровизация, искусственный интеллект.

Zamonaviy axborot texnologiyalarining rivojlanishi kiberjinoyatlarning nafaqat son jihatdan ortishiga, balki ularning mazmunan murakkablashishiga ham olib kelmoqda. Hozirgi kunda kiberjinoyatlar turli mezonlar asosida tasniflanayotgan bo’lib, xususan, Budapesht konvensiyasida ular quyidagi umumiy to’rtta guruhga: Kompyuter ma’lumotlari va tizimlarining maxfiyligi (Confidentiality), yaxlitligi

(Integrity) hamda mavjudligi (Availablity)ga qarshi jinoyatlar, Komyuter bilan bog'liq jinoyatlar, Kontent bilan bog'liq jinoyatlar (bolalar pornografiyasi bilan bo'g'liq jinoyatlar, Mualliflik huquqi va unga turdosh huquqlarning buzilishi bilan bog'liq jinoyatlar[1] ga ajratilgan bo'lsa-da, eng maqbul yondashuv sifatida ularni ikki asosiy guruhga ajratish mumkin: axborot texnologiyalariga qarshi qaratilgan kiberjinoyatlar va axborot texnologiyalari vositasida sodir etiladigan kiberjinoyatlar.

Birinchi guruhga kompyuter tizimlari va ma'lumotlar bazalariga bevosita zarar yetkazishga qaratilgan hujumlar kiradi. Bular jumlasiga noqonuniy kirish (hacking), ma'lumotlarni o'zgartirish yoki yo'q qilish, zararli dasturlar (malware) tarqatish, xizmat ko'rsatishni rad etish hujumlari (DDoS) hamda zaifliklardan foydalanishga asoslangan hujumlar (zero-day) kiradi. Ushbu turdagi kiberjinoyatlar asosan texnik infratuzilmani ishdan chiqarish yoki ma'lumotlarni egallashga qaratilganligi bilan ajralib turadi. . Masalan, Bu turdagi jinoyatlar Hindistoning "The Institute of Company Secretaries of India (ICSI)" instituti tomonidan taqdim qilingan "Cyber Crime: Laws and Practices" darsligida "Computer Target Cyber Crime" ya'ni "kompyuter nishon bo'lgan kiberjinoyatlar" deb keltirialdi va unga ko'ra bu turdagi jinoyatlarda asosiy zarar kompyuter tizimlari, ma'lumotlar bazalariga yetkaziladi, ular ishdan chiqariladi yoki ma'lumotlar ko'chirib olinadi, o'zgartiriladi yoxud boshqa usulda zararlanadi[2].

Ikkinchi guruh esa axborot texnologiyalari vositasida sodir etiladigan kiberjinoyatlar bo'lib, an'anaviy jinoyatlarning raqamli muhitda sodir etilishini ifodalaydi. Bunda kompyuter va internet vosita sifatida qo'llanilib, firibgarlik, phishing, identifikatsiya ma'lumotlarini o'g'irlash, onlayn moliyaviy jinoyatlar, noqonuniy kontent tarqatish kabi harakatlar amalga oshiriladi. Ushbu turdagi jinoyatlar ijtimoiy muhandislik usullariga tayangan holda inson omilidan faol foydalanilishi bilan xarakterlanadi. Misol uchun, Axborot texnologiyalari fani tadqiqotchisi Nottingam Universiteti professori Stiven Furnell bu kabi jinoyatlarga o'z asarida "Computer-enabled crimes" ya'ni "Kopmyuter vositasida vujudga keluvchi jinoyatlar" deb izoh berib o'tadi, unga ko'ra an'anaviy jinoyatlar kompyuter vositasida amalga oshirilishi ayanan shu turga kiradi[3]. Shu bilan birgalikda, Verzon kompaniyasining web-saytidagi 2023-yilgi ma'lumotlariga qaraganda, "ma'lumotlar buzilishi holatlarining 74%iga inson omili ya'ni fishing, bilmasdan xato qilib qo'yishi, ijtimoiy muhandislik va shu kabilar sabab bo'lgan"[4].

So'nggi yillarda kiberjinoyatlarning rivojlanish tendensiyalarida bir qator muhim o'zgarishlar kuzatilmoqda. Birinchidan, kiberjinoyatlar tobora avtomatlashtirilgan tus olmoqda. Sun'iy intellekt texnologiyalaridan foydalanish orqali fishing xabarlari, zararli dasturlar va hatto deepfake kontentlar yaratish imkoniyati kengaymoqda. Ikkinchidan, kiberjinoyatlar "xizmat sifatida" (Cybercrime-as-a-Service) modeliga o'tib, bu sohada maxsus "qora bozor" shakllanmoqda. Bu esa texnik bilimga ega bo'lmagan shaxslarning ham kiberjinoyat sodir etish imkoniyatini oshirmoqda. Uchinchidan, kiberjinoyatlarning transmilliy xarakteri kuchayib bormoqda. Jinoyatchilar bir davlat hududida turib boshqa davlatdagi tizimlarga hujum qilishi mumkinligi ularni aniqlash va javobgarlikka tortishni murakkablashtiradi. To'rtinchidan, moliyaviy texnologiyalar rivoji bilan bog'liq holda kriptovalyutalar orqali amalga oshiriladigan jinoyatlar soni ortib bormoqda, bu esa jinoiy daromadlarni yashirish imkoniyatini kengaytirmoqda. Europolning "Internet orqali sodir etiladigan uyushgan jinoyatlar

[1] Council of Europe, *Convention on Cybercrime (Budapest Convention)*, 3-10-moddalari, 2001.
[2] The Institute of Company Secretaries of India (ICSI). *Cyber Crime: Laws and Practices*. 2016, 4-bet.
[3] Steven Furnell. *Cybercrime: Vandalizing the Information Society*. London: Addison-Wesley – 2002, 22-bet.
[4] Verizon. *2023 Data Breach Investigations Report (DBIR)*. 2023. Ilmiy hisobot.

bo‘yicha tahdidni baholash 2024” (IOCTA 2024)[5] hisoboti hamda Jahon iqtisodiy forumi “WEF” tomonidan e’lon qilingan “Global kiberxavfsizlik istiqbollari 2025” (Global Cybersecurity Outlook 2025)[6] analitik hisobotlarida yuqoridagi fikrlar tasdig’i keltirilgan.

Bundan tashqari, pandemiya davridan keyin ijtimoiy munosabatlarning keng miqyosda raqamli shaklga o‘tishi kiberjinoyatlar uchun yangi imkoniyatlar yaratdi. Masofaviy ish, onlayn ta’lim va elektron tijoratning rivojlanishi foydalanuvchilar sonining keskin oshishiga olib kelib, bu esa kiberjinoyatchilar uchun yangi nishonlar paydo bo‘lishiga sabab bo‘ldi.

Tahlillar shuni ko‘rsatadiki, kiberjinoyatlar zamonaviy davrda murakkab, moslashuvchan va tez rivojlanayotgan hodisa sifatida namoyon bo‘lmoqda. Ularning turlari nafaqat ko‘payib bormoqda, balki texnologik taraqqiyot bilan uzviy bog‘liq holda sifat jihatidan ham o‘zgarib bormoqda. Ayniqsa, sun’iy intellekt, raqamli iqtisodiyot va global tarmoqlarning rivojlanishi kiberjinoyatlarning yangi shakllarini yuzaga keltirmoqda. Shu sababli, kiberjinoyatlarga qarshi kurashishda nafaqat texnik, balki huquqiy va tashkiliy choralarni ham kompleks tarzda takomillashtirish zarur.

FOYDALANILGAN ADABIYOTLAR RO’YXATI

1. Council of Europe, Convention on Cybercrime (Budapest Convention), 2001;
2. The Institute of Company Secretaries of India (ICSI). Cyber Crime: Laws and Practices. 2016;
3. Steven Furnell. Cybercrime: Vandalizing the Information Society. London: Addison-Wesley – 2002;
4. Verizon. 2023 Data Breach Investigations Report (DBIR). 2023. Ilmiy hisobot;
5. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Analitik hisobot. Luxembourg: Publications Office of the European Union, 2024.
URL:https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
6. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva: World Economic Forum, 2025. Analitik hisobot.
URL:https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[5] Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Analitik hisobot. Luxembourg: Publications Office of the European Union, 2024.
URL:https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

[6] World Economic Forum. *Global Cybersecurity Outlook 2025*. Geneva: World Economic Forum, 2025. Analitik hisobot. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf