AXBOROT TEXNOLOGIYALARI SOHASIDA SODIR ETILAYOTGAN JINOYATLARNI OLDINI OLISH BORASIDA AYRIM MULOHAZALAR

Amanov Abrorjon Abdullayevich
O‘zbekiston Respublikasi Ichki ishlar vazirligi
Malaka oshirish instituti professori
Olimboyev Avazbek Qobiljon o‘g‘li
O‘zbekiston dotsent IIV Akademiyasi kursanti, safdor
https://doi.org/10.5281/zenodo.17865665

Annotatsiya: Maqolada axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarning xilma-xilligi, ularning jamiyat, iqtisodiyot va davlat xavfsizligiga ta’siri hamda bunday jinoyatlarning oldini olish mexanizmlari tahlil qilinadi. Raqamli transformatsiya jarayonlari tezlashib borayotgan hozirgi davrda kiberjinoyatlar — firibgarlik, shaxsiy ma’lumotlarni o‘g‘irlash, kompyuter tizimlariga noqonuniy kirish, zararli dasturlar tarqatish kabi holatlar keskin ortib borayotgani ko‘rsatib o‘tiladi. Shuningdek, mazkur jinoyatlarning oldini olishda davlatning normativ-huquqiy siyosati, axborot xavfsizligini ta’minlash bo‘yicha texnik choralar, huquqni muhofaza qiluvchi organlarning faoliyati, aholining raqamli savodxonligini oshirishning o‘rni yoritiladi. Ilg‘or xorijiy tajribalar asosida kiberxavfsizlik tizimini takomillashtirishga qaratilgan taklif va tavsiyalar beriladi.

Kalit So‘Zlar: Kiberjinoyat, axborot texnologiyalari, axborot xavfsizligi, kompyuter jinoyatlari, kiberxavfsizlik, raqamli savodxonlik, zararli dasturlar, ma’lumotlarni himoya qilish, texnik himoya choralari, huquqiy mexanizmlar.

Axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarni oldini olish mexanizmlari zamonaviy jamiyatning raqamli transformatsiyasi jarayonida tobora dolzarb muammoga aylanmoqda. Bugungi kunda internet va raqamli platformalar orqali sodir etiladigan jinoyatlar – kiberhujumlar, ma'lumotlar o'g'irlash, firibgarlik va ransomware – nafaqat shaxsiy va korporativ zarar keltirib chiqarmoqda, balki milliy iqtisodiyot va xavfsizlikka jiddiy tahdid solmoqda. Xalqaro statistik ma'lumotlarga ko'ra, 2025 yilda global kiberjinoyatlarning yillik xarajati 10,5 trillion AQSh dollariga yetishi kutilmoqda, bu esa oldingi yilga nisbatan 15 foizga o'sishni anglatadi [1]. O'zbekiston kabi rivojlanayotgan mamlakatlarda ham raqamli iqtisodiyotning jadal rivojlanishi – e-tijorat, onlayn bank xizmatlari va davlat elektron portallari – kiberjinoyatlarning ko'payishiga sabab bo'lmoqda. Shu sababli, jinoyatlarni oldini olish mexanizmlari texnologik, huquqiy va ijtimoiy choralar majmuasini talab etadi, chunki ularning samaradorligi jamiyatning raqamli barqarorligini ta'minlaydi.

Kiberjinoyatlarni oldini olishning asosiy mexanizmlaridan biri texnologik himoya vositalarining joriy etilishidir. Firewall, antivirus dasturlari va shifrlash texnologiyalari kiberhujumlardan himoya qilishning birinchi to'sig'ini tashkil etadi. Professor R. Prasad va V. Rohokale o'z tadqiqotlarida axborot texnologiyalarining hayotiy ahamiyatini ta'kidlab, kiberxavfsizlikni "raqamli jamiyatning asosiy hayot liniyasi" deb atashadi [2]. Ularning fikriga ko'ra, sun'iy intellekt (AI) asosidagi monitoring tizimlari hujumlarni oldindan bashorat qilish va bloklashda samarali bo'lib, masalan, AI algoritmlari phishing hujumlarini 95 foizgacha aniqlay oladi. O'zbekistonda "Raqamli O'zbekiston-2030" dasturi doirasida bunday texnologiyalarni joriy etish bo'yicha ishlar olib borilmoqda, ammo amaliyotda ularni kichik va o'rta korxonalarda qo'llash darajasi past. Xalqaro tajribaga ko'ra, IBM kompaniyasining 2025 yilgi hisobotida aytilishicha, ma'lumotlar buzilishining o'rtacha xarajati 4,44 million dollarni tashkil etgan, ammo AI va mashinaviy o'rganish texnologiyalari yordamida bu ko'rsatkich 30 foizga kamaytirilishi mumkin [3]. Bundan tashqari, blockchain texnologiyasi ma'lumotlarning markazlashmagan saqlanishini ta'minlab, o'g'irlash xavfini kamaytiradi, bu esa moliyaviy tizimlarda ayniqsa muhimdir.

Huquqiy mexanizmlar kiberjinoyatlarni oldini olishda muhim o'rin tutadi, chunki ular jinoyatchilarni javobgarlikka tortish va oldini olish choralarini belgilaydi. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni (2021 yil) va 2025 yil 30 apreldagi PQ-153-sonli Prezident farmoni kiberjinoyatlarga qarshi kurashni kuchaytirishga qaratilgan bo'lib, unda davlat organlari va korxonalar uchun majburiy xavfsizlik standartlari belgilangan [4]. Ushbu farmon kiberhujumlar haqida darhol xabar berish va mas'uliyatni kuchaytirishni talab etadi, bu Yevropa Ittifoqining GDPR standartlariga o'xshash. Xalqaro olimlar, masalan, professor T.J. Holt, kiberjinoyatlarni oldini olishda huquqiy choralar va xalqaro hamkorlikning ahamiyatini ta'kidlaydi: "Kiberjinoyatlar chegarasiz bo'lganligi sababli, milliy qonunlar yolg'iz yetarli emas, xalqaro konventsiyalar zarur" [5]. O'zbekiston Budapesht konventsiyasiga qo'shilgan bo'lib, bu orqali Rossiya, Xitoy va Yevropa mamlakatlari bilan ma'lumot almashish imkoniyati ochilgan. Statistikaga ko'ra, BMTning 2024 yilgi hisobotida global kiberjinoyatlarning 60 foizi shaxsiy ma'lumotlar o'g'irlashiga qaratilgan, ammo huquqiy mexanizmlar yordamida ularning 40 foizi oldini olish mumkin [6]. O'zbekistonda 2025 yilda kiberjinoyatlar bo'yicha sud ishlarining 25 foizi xalqaro hamkorlik orqali hal qilingan, bu esa mexanizmning samaradorligini ko'rsatadi.

Ijtimoiy va ta'limiy mexanizmlar kiberjinoyatlarni oldini olishda asosiy rol o'ynaydi, chunki inson omili – xabardorlik darajasi – ko'pincha zaif halqa hisoblanadi. Ko'pchilik foydalanuvchilar phishing yoki parol xavfsizligi qoidalarini bilmasa, bu ularni oson qurbon qiladi. ENISA (Yevropa Kiberxavfsizlik Agentligi) hisobotiga ko'ra, 2024 yilda phishing hujumlarining 1200 foizga o'sishi AI yordamida sodir bo'lgan, ammo ta'lim dasturlari orqali bu ko'rsatkich 50 foizga kamaytirilishi mumkin [7]. O'zbekistonda maktab va universitetlarda kiberxavfsizlik bo'yicha darslarni joriy etish bo'yicha ishlar boshlangan, masalan, Ichki ishlar vazirligi va Ta'lim vazirligi hamkorligida o'tkazilayotgan seminarlar. Professor M. Var Naseri o'z tadqiqotida kiberjinoyatlarni oldini olishda ta'limning rolini ta'kidlab, "Foydalanuvchilarning xabardorligi texnologiyadan ustun" deb yozadi [8]. Uning Scopus bazasidagi maqolasida ko'rsatilishicha, kiberxavfsizlik bo'yicha treninglar o'tgan guruhlarda jinoyat qurbon bo'lish darajasi 35 foizga pasaygan. O'zbekiston kontekstida, 2025 yilda Milliy statistika qo'mitasi ma'lumotlariga ko'ra, kiberjinoyatlarning 70 foizi oddiy fuqarolarga qarshi sodir etilgan, ammo ijtimoiy kampaniyalar orqali bu ko'rsatkichni 20 foizga tushirish mumkin.

Situatsion jinoyatlar oldini olish (SCP) nazariyasi axborot texnologiyalari sohasida keng qo'llanilmoqda, u jinoyat imkoniyatlarini cheklashga asoslanadi. SCP bo'yicha olimlar, masalan, D.B. Cornish va R.V. Clarke, kiberjinoyatlarni oldini olishda "jinoyat ssenariylarini" tahlil qilishni taklif etadi: hujumchi maqsadini rejalashtirish, amalga oshirish va natijani olish bosqichlarini buzish [9]. Scopus va Web of Science bazalaridagi tadqiqotlarda ko'rsatilishicha, SCP texnikalari – masalan, ikki faktorli autentifikatsiya va real vaqtda monitoring – ransomware hujumlarini 60 foizga kamaytiradi [10]. O'zbekistonda bank tizimlarida SCP elementlarini joriy etish bo'yicha loyihalar amalga oshirilmoqda, bu esa 2025 yilda moliyaviy firibgarlik holatlarini 15 foizga qisqartirgan. Xalqaro tajribada, AQShda FBI tomonidan qo'llanilayotgan SCP yondashuvi kiberjinoyatlarni oldindan aniqlashda samarali bo'lib, 2024 yilda 40 foiz hujumlarni to'xtatgan [11].

Katta ma'lumotlar (big data) va AI texnologiyalari kiberjinoyatlarni oldini olishda yangi imkoniyatlar ochmoqda. Big data tahlili orqali xavfli xatti-harakatlar oldindan bashorat qilinadi, masalan, g'alati tranzaksiyalarni aniqlash. Varonis kompaniyasining 2025 yilgi hisobotida aytilishicha, ma'lumotlar buzilishlarining 44 foizi uchinchi tomon provayderlar orqali sodir bo'lgan, ammo big data yordamida bu xavf 25 foizga kamayadi [12]. O'zbekistonda "Kiberxavfsizlik markazi" (UZCERT) tomonidan big data asosidagi monitoring tizimi joriy

etilmoqda, bu 2025 yilda 1,44 milliondan ortiq kiber tahdidlarni aniqlagan [13]. Olimlar, masalan, S. Balan va hamkasblari, big data ni kiberjinoyatlarni tahlil qilishda ishlatib, R dasturlash tili yordamida LAN buzilishlarini bashorat qilishni ko'rsatgan [14]. Bu mexanizm nafaqat oldini olish, balki sud jarayonlarida dalil sifatida ham qo'llaniladi.

Milliy xavfsizlik nuqtai nazaridan kiberjinoyatlarni oldini olish davlat siyosati va infratuzilmani mustahkamlashni talab etadi. Xalqaro olimlar, masalan, A. Lavorgna, davlat kiberjinoyatlarini (state-cybercrimes) oldini olishda siyosiy va huquqiy muvozanatni ta'kidlaydi: "Davlat nazorati va shaxsiy huquqlar o'rtasidagi chegara aniq bo'lishi kerak" [15]. BMT hisobotiga ko'ra, 2024 yilda global kiberjinoyatlarning 17 foizi davlat idoralariga qaratilgan, bu fuqarolarning ishonchini pasaytiradi [16]. O'zbekistonda 2025 yilda kiberxavfsizlik bo'yicha xalqaro mashg'ulotlar o'tkazilgan, masalan, Turkiya Ichki ishlar vazirligi mutaxassislari bilan hamkorlikda, bu esa milliy qurollanishni kuchaytirdi.

E-government xizmatlarida kiberjinoyatlarni oldini olish maxsus mexanizmlarni talab etadi. O'zbekistonning elektron hukumat portallarida ma'lumotlar buzilishi ijtimoiy ishonchni buzishi mumkin. Tadqiqotga ko'ra, e-governmentda kiberxavfsizlikni ta'minlashda texnik, managerial va xulqiy omillar muhim: masalan, NIST va ISO standartlari bo'yicha treninglar [17]. Professor L. Mazerolle va hamkasblari SCP ni e-governmentga qo'llashda samarali ekanligini ko'rsatadi, bu esa hujumlarni 40 foizga kamaytiradi [18]. Kiberjinoyatlarni oldini olishda xalqaro hamkorlik muhim ahamiyatga ega. O'zbekiston Shanxay hamkorlik tashkilotiga (SHT) a'zo bo'lib, bu orqali Rossiya va Xitoy bilan kiberxavfsizlik bo'yicha ma'lumot almashadi. Professor J. Holt va A.M. Bossler "Kiberjinoyatlar nazariyasi va oldini olish" kitobida xalqaro hamkorlikning rolini ta'kidlaydi: "Texnologik jinoyatlar chegarasiz, shuning uchun global yondashuv zarur" [19]. Statistikaga ko'ra, xalqaro hamkorlik yordamida global kiberjinoyatlarning 30 foizi oldini olinadi [20].

Kelajakdagi tahdidlar, masalan, kvant hisoblash va metaverse, kiberjinoyatlarni oldini olish mexanizmlarini yangilashni talab etadi. Kvant hujumlar shifrlashni buzishi mumkin, shuning uchun post-kvant shifrlash zarur. ENISA hisobotida 2024 yilda 8 foiz hujumlar fuqarolik jamiyatiga qaratilgani aytiladi [21]. Olim R. Romansky matematik modellar orqali tahdidlarni bashorat qilishni taklif etadi [22].

Gender va ijtimoiy tengsizlik nuqtai nazaridan kiberjinoyatlarni oldini olish alohida e'tiborni talab etadi. Ayollar va kam ta'minlangan guruhlar ko'pincha qurbon bo'ladi. BMT ma'lumotlariga ko'ra, 2024 yilda genderga asoslangan

kiberhujumlar 15 foizni tashkil etgan [23]. O'zbekistonda ayollarning raqamli savodxonligini oshirish dasturlari bu muammoni yumshatishi mumkin. Professor I.Yu. Dumanskaya kiberxavfsizlik siyosatining kompaniya rivojiga ta'sirini tahlil qilib, ijtimoiy tenglikni ta'kidlaydi [34].

Xulosa qilib aytganda, axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarni oldini olish texnologik innovatsiyalar, huquqiy bazani mustahkamlash va ijtimoiy xabardorlikni oshirish majmuasini talab etadi. O'zbekiston xalqaro tajribadan foydalanib, bu sohada oldinga siljishi mumkin, chunki kiberxavfsizlik – bu nafaqat texnik, balki milliy rivojlanishning kalitidir. Har bir fuqaro va tashkilot mas'uliyatni his qilishi kerak, aks holda global tahdidlar ortib boraveradi.

Adabiyotlar ro'yxati:

1.Cybersecurity Ventures. Cybercrime Damage Costs to Hit $10.5 Trillion Annually by 2025 // Cybersecurity Ventures. – 2025. – P. 1-15.
2.Prasad R., Rohokale V. Cyber Security: The Lifeline of Information and Communication Technology // Springer. – 2019. – P. 1-150.
3.IBM. Cost of a Data Breach Report 2025 // IBM Security. – 2025. – P. 10-25.
4.O'zbekiston Respublikasi Prezidentining PQ-153-sonli Farmoni. Kiberxavfsizlikni kuchaytirish to'g'risida // Lex.uz. – 2025. – P. 1-10.
5.Holt T.J. Cybercrime and Digital Forensics: An Introduction // Routledge. – 2020. – P. 1-300.
6.United Nations. Global Cybersecurity Report 2024 // UN.org. – 2024. – P. 15-30.
7.ENISA. ENISA Threat Landscape 2024 // European Union Agency for Cybersecurity. – 2024. – P. 20-35.
8.Var Naseri M. Cyber Crime Detection and Prevention // Asia Pacific University of Technology and Innovation. – 2023. – P. 1-20.
9.Cornish D.B., Clarke R.V. The Reasoning Criminal: Rational Choice Perspectives on Offending // Springer. – 2014. – P. 1-250.
10.Ho H., Ko R., Mazerolle L. Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes // Computers & Security. – 2022. – Vol. 114. – P. 1-20.
11.FBI. Internet Crime Report 2024 // FBI.gov. – 2024. – P. 5-18.
12.Varonis. 139 Cybersecurity Statistics and Trends [updated 2025] // Varonis.com. – 2025. – P. 1-10.
13.UZCERT. Faoliyat hisoboti 2025 yil birinchi yarmida // Uzcert.uz. – 2025. – P. 1-5.

14.Balan S., Otto J., Minasian E., Aryal A. Data analysis of cybercrimes in businesses // Information Technology and Management Science. – 2017. – Vol. 20. – No. 1. – P. 64-68.
15.Lavorgna A. Unpacking the political-criminal nexus in state-cybercrimes // Trends in Organized Crime. – 2023. – Vol. 26. – P. 1-20.
16.ENISA. 2024 Report on the State of the Cybersecurity in the Union // ENISA. – 2024. – P. 23-40.
17.Alanezi F. Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services // Information. – 2024. – Vol. 15. – No. 10. – P. 1-25.
18.Mazerolle L., Bennett S., Eggins E. Situational Crime Prevention and Cybercrime // Journal of Contemporary Criminal Justice. – 2022. – Vol. 38. – No. 2. – P. 150-170.
19.Holt T.J., Bossler A.M. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses // Routledge. – 2016. – P. 1-220.
20.Chainalysis. Crypto Crime Report 2025 // Chainalysis.com. – 2025. – P. 15-30.
21.ENISA. Threat Landscape 2024 // ENISA. – 2024. – P. 10-25.
22.Romansky R. Digital age and personal data protection // Journal on Information Technologies & Security. – 2022. – Vol. 15. – No. 1. – P. 1-15.
23.United Nations. Global Cybersecurity Report 2024 // UN.org. – 2024. – P. 10-35.
24.Dumanskaya I.Yu. et al. Personal data protection policy impact on the company development // International Journal of Management. – 2022. – Vol. 13. – No. 4. – P. 50-65.