# HIDDEN THREATS OF THE DIGITAL WORLD: WHY IS CYBERCRIME INCREASING RAPIDLY?

**Vohidjonov Muhammadali Sherzod o‘g‘li**
Student of Group 204 Namangan Regional Academic Lyceum under Tashkent State University of Law
E-mail: vohidjanov2007@gmail.com
**Qodirjonov Axidillo Axmadjon o‘g‘li**
Student of Group 204 Namangan Regional Academic Lyceum under Tashkent State University of Law
E-mail: axidilloqodirjanov@gmail.com

**Annotation**

This article provides an in-depth analysis of the sharp rise in cybercrime amid the rapid development of digital technologies and the internet. It examines the causes, main forms, global and national statistics, and consequences of cybercrime. Particular attention is paid to artificial intelligence (AI), ransomware, phishing, deepfakes, and other threats. The paper highlights the 11-fold increase in cybercrimes in Uzbekistan, trillions of soums in losses to citizens, and state measures. Practical recommendations for strengthening cybersecurity are offered.

**Keywords:** cybercrime, digital threats, ransomware, phishing, artificial intelligence, deepfake, cybersecurity, Uzbekistan, AI attacks.

# RAQAMLI DUNYONING YASHIRIN TAHDIDLARI: KIBERJINOYATCHILIK NEGA KESKIN ORTMOQDA?

Vohidjonov Muhammadali Sherzod o‘g‘li
TDYU huzuridagi Namangan viloyat akademik litseyining 204-guruh o’quvchisi
vohidjanov2007@gmail.com
Qodirjonov Axidillo Axmadjon o’g’li

TDYU huzuridagi Namangan viloyat akademik litseyining 204-guruh o'quvchisi
axidilloqodirjanov@gmail.com

Annotatsiya

Ushbu maqola raqamli texnologiyalar va internetning jadal rivojlanishi sharoitida kiberjinoyatchilikning keskin ortishi sabablari, asosiy ko'rinishlari, global va milliy statistikasi hamda oqibatlarini chuqur tahlil qiladi. Sun'iy intellekt (AI), ransomware, phishing, deepfake va boshqa tahdidlar batafsil ko'rib chiqiladi. O'zbekistonda kiberjinoyatlarning 11 baravar o'sishi, fuqarolarning trillion so'mlik zarar ko'rishi va davlat choralariga alohida e'tibor qaratilgan. Maqola kiberxavfsizlikni kuchaytirish bo'yicha amaliy tavsiyalar beradi.

Kalit so'zlar (O'zbekcha): kiberjinoyatchilik, raqamli tahdidlar, ransomware, phishing, sun'iy intellekt, deepfake, kiberxavfsizlik, O'zbekiston, AI hujumlari.

Аннотация

В данной статье проводится глубокий анализ резкого роста киберпреступности в условиях быстрого развития цифровых технологий и интернета. Рассматриваются причины, основные формы, глобальная и национальная статистика, а также последствия киберпреступности. Особое внимание уделяется искусственному интеллекту (ИИ), ransomware, фишингу, дипфейкам и другим угрозам. Подчеркивается 11-кратный рост киберпреступлений в Узбекистане, триллионные потери граждан и государственные меры. Предлагаются практические рекомендации по усилению кибербезопасности.

Ключевые слова: киберпреступность, цифровые угрозы, ransomware, фишинг, искусственный интеллект, дипфейк, кибербезопасность, Узбекистан, ИИ-атаки.

XXI asrning ikkinchi choragida insoniyat hayoti raqamli texnologiyalarsiz tasavvur qilib bo'lmaydi. Internet, smartfonlar, sun'iy intellekt, IoT qurilmalari va bulutli hisoblash tizimlari iqtisodiyot, ta'lim, sog'liqni saqlash va davlat boshqaruvini tubdan

o‘zgartirdi. Biroq bu rivojlanish bilan birga yangi, yashirin va juda xavfli tahdidlar paydo bo‘ldi. Kiberjinoyatchilik zamonaviy jamiyatning eng jiddiy muammolaridan biriga aylandi.[1]

Cybersecurity Ventures ma’lumotlariga ko‘ra, 2025-yilda global kiberjinoyatchilik zararini yiliga 10,5 trillion AQSH dollariga yetgan. Bu ko‘rsatkich AQSh va Xitoydan keyin uchinchi o‘rinda turadigan “iqtisodiyot”ga teng.[2] Agar kiberjinoyatchilik alohida davlat bo‘lsa, u dunyodagi eng yirik iqtisodiyotlar qatoriga kirardi.

O‘zbekistonda vaziyat yanada keskin. Ichki ishlar vazirligi ma’lumotlariga ko‘ra, 2021–2025-yillarda kiberjinoyatlar soni 11 baravarga ortib, 4865 tadan 62 440 taga yetgan. [3]2025-yilning o‘zida fuqarolar 1 trillion 890 milliard so‘m zarar ko‘rgan. Umumiy 5 yillik zarar esa 3,73 trillion so‘mni tashkil etgan. Kiberjinoyatlar barcha jinoyatlarning deyarli yarmiga yetgan.

Ushbu maqolada kiberjinoyatchilikning ortish sabablari, asosiy turlari, statistikasi va unga qarshi kurash choralarini batafsil yoritamiz.

Kiberjinoyatchilikning keskin ortishiga asosiy sabablar

Kiberjinoyatchilikning jadal o‘sishiga bir nechta omillar majmuasi ta’sir qilmoqda:

1. Raqamli transformatsiyaning tez sur’atlari

Internet foydalanuvchilar sonining ortishi, bank operatsiyalarining to‘liq raqamlashtirilishi, davlat xizmatlarining onlayn ko‘rsatilishi va IoT qurilmalari keng tarqalishi hujum uchun ulkan maydon yaratdi. Bulutli xizmatlar va 5G tarmoqlari yangi zaifliklarni keltirib chiqarmoqda.[4]

2. Sun’iy intellektning jinoyatchilar qo‘lida qurolga aylanishi

[1] 1. Cybersecurity Ventures. (2025). Cybercrime To Cost the World $10.5 Trillion Annually By 2025.

[2] . O‘zbekiston Respublikasi Ichki ishlar vazirligi. (2025). Kiberjinoyatchilik statistikasi hisoboti.
[3] UZCERT. (2025). 2025-yil uchun O‘zbekistonda asosiy kiber tahdidlar prognozi.
[4] World Economic Forum. Global Cybersecurity Outlook 2026.

Generativ AI (ChatGPT kabi modellar) jinoyatchilarga mukammal phishing xabarlarini yozish, deepfake video va ovoz klonlash imkonini beradi. 2025-yilda phishing hujumlarining 80% ga yaqini AI yordamida yaratilgan. AI-powered phishing ochilish darajasi an'anaviy hujumlarga nisbatan ikki baravar yuqori. Ovoz va video deepfake'lar orqali "CEO fraud" (rahbar impersonatsiyasi) holatlari keskin oshgan.

3. Crime-as-a-Service (CaaS) modeli

Darkweb'da Ransomware-as-a-Service (RaaS), phishing kitlari va boshqa vositalarni ijaraga olish mumkin. Bu yangi boshlovchi jinoyatchilarga ham katta miqyosli hujumlar uyushtirish imkonini beradi.

4. Foydalanuvchilar va tashkilotlarning past tayyorgarligi

Ko'pchilik parol himoyasi, ikki faktorli autentifikatsiya (2FA) va ijtimoiy injeneriya usullarini tan olish bo'yicha yetarli bilimga ega emas. Ijtimoiy tarmoqlar orqali tarqaladigan firibgarliklar hali ham eng samarali usul hisoblanadi.

5. Geosiyosiy omillar va davlat homiyligi

Ba'zi davlatlar kiberhujumlarni strategik qurol sifatida ishlatmoqda. Shuningdek, kriptovalyuta va anonim to'lov tizimlari jinoyatchilarga pulni yashirish imkonini beradi.[5]

Asosiy kiber tahdid turlari va ularning mexanizmlari

- Ransomware (tovlamachilik dasturlari): Ma'lumotlarni shifrlab, to'lov talab qilish. 2025-yilda ransomware hujumlari 149% ga oshgan. Double extortion (ma'lumotni o'g'irlash + shifrlash) usuli keng tarqalgan. O'rtacha to'lov miqdori o'sib bormoqda.
- Phishing, smishing va vishing: Email, SMS yoki qo'ng'iroq orqali shaxsiy ma'lumotlar va parollarni o'g'irlash. AI bu xabarlarni shaxsiy va ishonchli qiladi.

[5] . SpecialEurasia. (2025). Rising Cybercrime Alarms Uzbekistan's National Security.

- Deepfake va ovoz klonlash: Bank xodimi yoki yaqin qarindosh sifatida video/qo‘ng‘iroq orqali pul o‘tkazishni talab qilish. 2025-yilda deepfake hujumlari keskin oshgan.

- Business Email Compromise (BEC) va investitsiya firibgarliklari: Rahbar nomidan xat yuborib, katta miqdorda pul o‘tkazishni so‘rash.[6]

- Ma’lumotlar o‘g‘irlash (Data Breach) va identifikatsiya o‘g‘irlashi: Olingan ma’lumotlar darkweb’da sotiladi.

O‘zbekistonda banking sektoriga qaratilgan phishing va fuqarolarga qarshi firibgarliklar ustunlik qilmoqda.

Global va milliy statistika

Global miqyosda:

- 2025-yilda kiberjinoyatchilik zarari — 10,5 trillion dollar.

- FBI IC3 hisobotiga ko‘ra, 2025-yilda AQShda zarar 21 milliard dollardan oshgan.

- Har 39 soniyada biror tashkilotga hujum sodir bo‘lmoqda.

O‘zbekistonda:

- 2021–2025-yillarda jinoyatlar 11 baravar oshgan. [7]

- 2025-yilda fuqarolarga yetkazilgan zarar — “1,89 trillion” so‘m.

- Yoshlar (14–30 yosh) eng ko‘p qurbon bo‘lmoqda.

- Davlat 2025-yilda kiberxavfsizlik bo‘yicha maxsus farmon (PQ-153) qabul qildi.

Kiberjinoyatchilikning iqtisodiy, ijtimoiy va siyosiy oqibatlari

Moliyaviy zarar bilan birga infratuzilma (elektr tarmoqlari, sog‘liqni saqlash) to‘xtab qolishi, milliy xavfsizlikka tahdid va jamiyatdagi ishonchsizlik muammolari kuchaymoqda. Yoshlar orasida kiberzo‘ravonlik va onlayn firibgarlik psixologik bosim yaratmoqda.

[6] FBI Internet Crime Complaint Center (IC3) Report 2025.
[7] Rapid7. Emerging Trends in AI-Related Cyberthreats in 2025.

Xulosa va amaliy takliflar

Kiberjinoyatchilikni to‘liq yo‘q qilib bo‘lmaydi, ammo uning zararini keskin kamaytirish mumkin. Quyidagi choralar zarur:

- Fuqarolar, ayniqsa yoshlar orasida kiberxavfsizlik savodxonligini oshirish (maktab va universitet darslariga kiritish).
- Davlat va banklar tomonidan doimiy ogohlantirish kampaniyalari.
- Zamonaviy himoya vositalari (AI-based defense, zero-trust arxitekturasi) joriy etish.
- Xalqaro hamkorlikni kuchaytirish (INTERPOL, Europol bilan).
- Qonunchilikni takomillashtirish va jinoyatchilarni javobgarlikka tortishni oshirish.

Raqamli dunyo bizga ulkan imkoniyatlar beradi, ammo uning yashirin tahdidlarini e’tiborsiz qoldirib bo‘lmaydi. Har bir fuqaro, kompaniya va davlat o‘z darajasida mas’uliyatni his qilishi kerak. Faqat birgalikdagi sa’y-harakatlar bilan bu tahdidlarga qarshi samarali kurashish mumkin.

Adabiyotlar

1. Cybersecurity Ventures. (2025). Cybercrime To Cost the World $10.5 Trillion Annually By 2025.
2. O‘zbekiston Respublikasi Ichki ishlar vazirligi. (2025). Kiberjinoyatchilik statistikasi hisoboti.
3. UZCERT. (2025). 2025-yil uchun O‘zbekistonda asosiy kiber tahdidlar prognozi.
4. World Economic Forum. Global Cybersecurity Outlook 2026.
5. SpecialEurasia. (2025). Rising Cybercrime Alarms Uzbekistan's National Security.
6. FBI Internet Crime Complaint Center (IC3) Report 2025.
7. Rapid7. Emerging Trends in AI-Related Cyberthreats in 2025.