ICHKI ISHLAR ORGANLARINING KIBERJINOYATLARNI OLDINI OLISHDA DAVLAT ORGANLARI, MUASSASA VA TASHKILOTLAR BILAN O'ZARO HAMKORLIGI

Idiyev Jamshid Jafarovich
O‘zbekiston Respublikasi IIV Akademiyasi kursanti
Iminov Abdurasul Abdulatipovich
O‘zbekiston Respublikasi IIV Akademiyasi Raqamli va texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i, matematika va fizika fanlari nomzodi

Annotatsiya: *Mazkur maqolada ichki ishlar organlarining kiberjinoyatlarni oldini olishdagi o‘rni hamda bu jarayonda davlat organlari, muassasa va tashkilotlar bilan o‘zaro hamkorlik mexanizmlari tahlil qilingan. Kiberjinoyatlarning zamonaviy turlari, ularning jamiyat va davlat xavfsizligiga ta’siri yoritilib, ularni bartaraf etishda axborot almashinuvi, normativ-huquqiy bazani takomillashtirish va texnik imkoniyatlarni rivojlantirishning ahamiyati asoslab berilgan. Shuningdek, bank-moliya sektori, telekommunikatsiya kompaniyalari, ta’lim muassasalari hamda xalqaro tashkilotlar bilan hamkorlikning muhim jihatlari ko‘rib chiqilgan. Maqolada kiberjinoyatlarning oldini olishga qaratilgan profilaktik choralar va mavjud muammolarni bartaraf etish yo‘llari yuzasidan takliflar ilgari surilgan.*

Kalit so’zlar*: Kiberjinoyatchilik, kiberxavfsizlik, profilaktika,davlat organlari bilan hamkorlik, davlat-xususiy hamkorlik, axborot xavfsizligi, kibertahdidlar, axborot almashinuvi, ma’lumotlarni himoya qilish.*

Annotation: *This article analyzes the role of internal affairs bodies in preventing cybercrimes and the mechanisms of interaction with state bodies, institutions and organizations in this process. Modern types of cybercrimes, their impact on society and state security are highlighted, and the importance of information exchange, improvement of the regulatory framework and development of technical capabilities in eliminating them is substantiated. Also, important aspects of cooperation with the banking and financial sector, telecommunications companies, educational institutions and international organizations are considered. The article puts forward proposals for preventive measures aimed at preventing cybercrimes and ways to eliminate existing problems. Keywords: Cybercrime, cybersecurity, prevention, cooperation with state bodies, public-private cooperation, information security, cyber threats, information exchange, data protection. This article will serve as a useful resource for researchers, students and practicing specialists conducting scientific research in the field of cybersecurity.*

Raqamli texnologiyalarning jadallik bilan rivojlanishi bilan kiberjinoyatchilik global va milliy xavfsizlikka jiddiy tahdidga aylandi. 2025 yilga kelib, jahon bo‘yicha kiberjinoyatchilikdan kelgan zarar 10,5 trillion dollarga yetishi kutilmoqda. O‘zbekistonda esa so‘nggi besh yil ichida kiberjinoyatlar soni 11 barobarga o‘sib, 2025 yilda Toshkent shahrida qayd etilgan

jinoyatlarning yarimidan ko‘pi kiberhujumlar hisoblanadi. Fuqarolar va kompaniyalarga yetkazilgan moddiy zarar 2025 yilning birinchi 11 oyida 1,89 trillion so‘mdan oshdi.

Bunday sharoitda davlat va xususiy sektor o‘rtasidagi hamkorlik (Public-Private Partnership — PPP) samarali profilaktikaning asosiy kalitiga aylanadi. Davlat qonunchilik va huquqni muhofaza qilish imkoniyatlariga ega bo‘lsa, xususiy sektor innovatsion texnologiyalar, real vaqtdagi ma’lumotlar va tez javob berish qobiliyati bilan ajralib turadi.

Hamkorlikning asosiy yo‘nalishlari va ahamiyati

1. Axborot almashish va tahdidlarni erta aniqlash Kiberhujumlar ko‘pincha xususiy kompaniyalar tizimlarida boshlanadi. Ularning ma’lumotlari davlat idoralariga o‘z vaqtida yetkazilsa, milliy miqyosda himoya choralari ko‘riladi.

AQSh misolida CISA (Cybersecurity and Infrastructure Security Agency) tashkil etgan Joint Cyber Defense Collaborative (JCDC) platformasi davlat va yirik texnologiya kompaniyalari (Microsoft, Google, CrowdStrike va boshqalar) o‘rtasidagi hamkorlikning yorqin namunasidir. Log4j zaifligi kabi global tahdidlarga qarshi ushbu hamkorlik samarali javob berishni ta’minladi.

O‘zbekistonda ham UZCERT va xususiy telekom, bank va IT-kompaniyalar o‘rtasida shunday mexanizmlarni rivojlantirish dolzarbdir.

2. Texnologiyalar va infratuzilmani himoya qilish Xususiy sektor kiberhimoya bo‘yicha eng ilg‘or yechimlarni ishlab chiqadi. Masalan, 2025 yilda O‘zbekiston Palo Alto Networks kompaniyasi bilan strategik shartnoma imzoladi. Ushbu hamkorlik davlat va xususiy sektorning ma’lumotlarni himoya qilish tizimlariga sun’iy intellektga asoslangan texnologiyalarni joriy etishga qaratilgan.

3. Qonunchilik va me’yorlarni takomillashtirish Davlat qonunlarni qabul qiladi, xususiy sektor esa ularning amaliyotda qanday ishlashi haqida fikr beradi. Banklar, telekommunikatsiya kompaniyalari va IT-firmalarining ishtirokida ishlab chiqilgan standartlar samaraliroq bo‘ladi.

4. Kadrlar tayyorlash va savodxonlikni oshirish Hamkorlik orqali o‘quv dasturlari, seminarlar va simulyatsiya mashg‘ulotlari tashkil etiladi. Xususiy kompaniyalar mutaxassislarining davlat idoralari xodimlarini o‘qitishi mumkin.

5. Xalqaro hamkorlikda ishtirok Davlat-xususiy hamkorlik xalqaro platformalarda (INTERPOL, UNODC va boshqalar) kuchliroq pozitsiya beradi.

O‘zbekistondagi holat va imkoniyatlar

O‘zbekiston “Raqamli O‘zbekiston-2030” strategiyasi doirasida kiberxavfsizlikni mustahkamlashga jiddiy e’tibor qaratmoqda. 2026–2030 yillarga mo‘ljallangan milliy kiberxavfsizlik strategiyasi qabul qilingan. Biroq, hamkorlik mexanizmi hali to‘liq shakllanmagan.

Mavjud muammolar:

Axborot almashishning yetarlicha samarali kanallari yo‘q.

Xususiy sektorning ishtiroki cheklangan.

Ishonch va qonuniy himoya mexanizmlarining yetishmasligi.

Milliy kiberxavfsizlik kengashi tashkil etish (davlat, bank, telekom, IT va xususiy sektor vakillari).

Axborot almashish to‘g‘risidagi qonunchilikni takomillashtirish (anonimlashtirilgan ma’lumotlarning himoyasi).

Qo‘shma simulyatsiya mashg‘ulotlari va “Red Team” mashqlarini o‘tkazish.

Xususiy sektorga imtiyozlar berish (kiberhimoya texnologiyalarini joriy etishda soliq yengilliklari).

Davlat va xususiy sektor hamkorligi — bu davlat organlari hamda xususiy kompaniyalar o‘rtasidagi uzoq muddatli strategik hamkorlik bo‘lib, u kiberxavfsizlikni ta'minlash, tahdidlarni bartaraf etish va axborot almashinuvini kuchaytirishga qaratilgan.

Tadqiqotlarga ko‘ra, zamonaviy infratuzilmaning katta qismi xususiy sektorga tegishli bo‘lib, masalan, ayrim davlatlarda muhim infratuzilmaning taxminan 80–85% qismi xususiy tashkilotlar tomonidan boshqariladi . Shuning uchun davlat yakka holda barcha kibertahdidlarni bartaraf eta olmaydi.

Kiberjinoyatchilikni oldini olishda davlat va xususiy sektor hamkorligi quyidagi yo‘nalishlarda muhim ahamiyatga ega:

Axborot almashinuvi

Kibertahdidlar haqidagi ma'lumotlarni tezkor almashish orqali hujumlarni erta aniqlash va bartaraf etish mumkin. Agar kompaniyalar o‘zlari duch kelgan tahdidlar haqida ma'lumot bermasa, umumiy xavfsizlik muhiti zaiflashadi .

Resurs va bilimlarni birlashtirish

Davlat — huquqiy vakolatlarga ega, xususiy sektor esa texnologiya va innovasiyalarda yetakchi hisoblanadi. Ularning hamkorligi natijasida samarali himoya tizimi shakllanadi .

Real vaqtda monitoring va profilaktika

Hamkorlik asosida yaratilgan platformalar orqali tahdidlarni real vaqtda kuzatish va ularni oldini olish imkoni paydo bo‘ladi.

Kiberxavfsizlik sohasida davlat va xususiy sektor hamkorligi quyidagi shakllarda amalga oshiriladi:

Qo‘shma kiberxavfsizlik markazlari tashkil etish

Tahdidlar bo‘yicha axborot bazalarini shakllantirish

Kiberxavfsizlik bo‘yicha standartlar va qonunchilikni ishlab chiqish

Kadrlar tayyorlash va trening dasturlari

Mutaxassislar ta'kidlashicha, kiberxavfsizlik — “jamoaviy jarayon” bo‘lib, hech bir tashkilot barcha ma'lumotga ega emas .

Xalqaro amaliyotda davlat va xususiy sektor hamkorligi kiberjinoyatchilikka qarshi kurashda asosiy vosita sifatida qaraladi. Masalan:

Yevropa Ittifoqida kiberxavfsizlik strategiyalari doirasida davlat va xususiy sektor o‘rtasida axborot almashinuvi tizimi yo‘lga qo‘yilgan

AQShda maxsus hamkorlik markazlari orqali davlat va biznes birgalikda kibertahdidlarga qarshi choralar ko‘radi

Kichik va o‘rta biznes sub'ektlarini himoya qilish uchun davlat tomonidan qo‘llab-quvvatlash dasturlari ishlab chiqilgan

Hamkorlik samarali bo‘lishiga qaramay, qator muammolar ham mavjud:

Ishonch yetishmasligi

Axborotni maxfiy saqlash muammosi

Standartlarning turlicha bo‘lishi

Kadrlar yetishmasligi

Bu muammolarni hal qilish uchun:

huquqiy bazani takomillashtirish

yagona standartlar joriy qilish

axborot almashinuvini rag‘batlantirish

doimiy hamkorlik platformalarini yaratish zarur

Xulosa qilib aytganda, kiberjinoyatchilikni oldini olishda davlat va xususiy sektor hamkorligi hal qiluvchi omil hisoblanadi. Zamonaviy raqamli muhitda hech bir tashkilot yoki davlat yakka holda kibertahdidlarga qarshi samarali kurasha olmaydi. Shuning uchun resurslar, texnologiyalar va bilimlarni birlashtirish orqali kompleks yondashuvni shakllantirish zarur. Kiberjinoyatchilikka qarshi kurashda davlat va xususiy sektor hamkorligi — bu tanlov emas, balki zaruriyatdir. Bir tomonlama harakatlar samarasiz. Faqat ishonchga asoslangan, qonuniy va texnologik jihatdan qo‘llab-quvvatlangan hamkorlik orqaligina raqamli iqtisodiyotni himoya qilish va fuqarolarning ishonchini saqlash mumkin.

O‘zbekiston bu yo‘lda ilg‘or davlatlar tajribasidan (AQSh, Estoniya, Singapur) foydalanib, o‘ziga xos milliy modelni yaratishi mumkin. Bu nafaqat kiberhujumlar sonini kamaytiradi, balki mamlakatning raqamli transformatsiyasining barqarorligini ta’minlaydi.

F O Y D A L A N I L G A N A D A B I Y O T L A R:

1. O‘zbekiston Respublikasining Qonuni – “Kiberxavfsizlik to’g’risida”, O‘RQ – 764, 15.04.2022-yil

2. Abduraximov B.F. (professor). Kiberxavfsizlik va kriminalistika: Raqamli dalillarni tahlil qilish usullari. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti nashriyoti. 2023 y. (Kiberjinoyatlarda raqamli dalillarning o'ziga xosligi va forensika usullari).

3. UzCERT. Uzbekistan strengthened its position in the Global Cyber Security Index. 10.10.2025 y. (Kiberxavfsizlik hodisalari statistikasi)

4. ISO. ISO/IEC 27037:2012 – Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012 y.

5. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi materiallari.

6. Wikipediya onlayn erkin ensiklopediyasi - https://uz.wikipedia.org

7. Christopher Hadnagy - Social Engineering: The Science of Human Hacking - 2018