KIBERXAVF MONITORINGI VA UNI HUQUQIY TARTIBGA SOLISHNING DOLZARB MASALALARI

Quvvatova Kumush Mo'min qizi
Tashkent international university "Yurispuridensiya" yo'nalishi
3-kurs talabasi
kumushquvvatova19@gmail.com

Annotatsiya: Mazkur maqolada kiberxavflarni monitoring qilishning huquqiy asoslari, davlat axborot tizimlarining xavfsizligini ta'minlash mexanizmlari va ushbu jarayonni tartibga soluvchi normativ-huquqiy hujjatlar tahlil qilinadi. Tadqiqot davomida kiberxavfsizlik monitoringining preventiv ahamiyati, muhim axborot infratuzilmasi ob'ektlarini himoya qilishdagi roli hamda kiberhodisalarga huquqiy munosabat bildirishning zamonaviy usullari o'rganilgan. Maqola yakunida milliy qonunchilikni takomillashtirish bo'yicha ilmiy asoslangan tavsiyalar ilgari surilgan.

Kalit so'zlar: kiberxavfsizlik, monitoring, huquqiy asoslar, axborot infratuzilmasi, kiberjinoyatchilik, raqamli dalil, ma'lumotlar himoyasi, kiber-audit, milliy xavfsizlik, preventiv choralar.

Аннотация: В данной статье рассматриваются правовые основы мониторинга киберугроз, механизмы обеспечения безопасности национальных информационных систем и роль государственного регулирования в этой сфере. Анализируются методы выявления киберинцидентов и их правовое значение в системе обеспечения национальной безопасности. В статье представлены предложения по совершенствованию законодательства в области защиты критической информационной инфраструктуры.

Ключевые слова: кибербезопасность, мониторинг, правовые основы, информационная инфраструктура, киберпреступность, цифровое доказательство, защита данных, кибераудит, национальная безопасность, превентивные меры.

Abstract: This article discusses the legal foundations of cyber threat monitoring, the mechanisms for ensuring the security of national information systems, and the role of state regulation in this field. It analyzes methods for identifying cyber incidents and their legal significance within the national security framework. The article presents proposals for improving legislation regarding the protection of critical information infrastructure.

Key words: cybersecurity, monitoring, legal framework, information infrastructure, cybercrime, digital evidence, data protection, cyber audit, national security, preventive measures.

Kirish

Insoniyat taraqqiyotining hozirgi bosqichida axborot texnologiyalari jamiyat hayotining barcha jabhalariga chuqur kirib bordi. Biroq, raqamlashtirish jarayonining jadallashuvi bilan birga kibertahdidlar ko‘lami va murakkabligi ham ortib bormoqda. Kiberxavflarni monitoring qilish — bu nafaqat texnik jarayon, balki davlatning suvereniteti va fuqarolarning huquqlarini himoya qilishga qaratilgan huquqiy institutdir. O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlashning huquqiy asoslarini yaratish va monitoring tizimini qonuniy tartibga solish milliy xavfsizlikning ustuvor yo‘nalishlaridan biri hisoblanadi.

Kiberxavf monitoringi deganda, axborot tizimlari va resurslarida yuzaga kelishi mumkin bo‘lgan tahdidlarni barvaqt aniqlash, ularni baholash va real vaqt rejimida kuzatib borish tushuniladi.

Huquqiy nuqtai nazardan monitoring ikki xil xarakterga ega:

1. **Majburiy monitoring:** Muhim axborot infratuzilmasi (MAI) ob'ektlari uchun qonun bilan belgilangan talab.
2. **Ixtiyoriy monitoring:** Xususiy sektor sub'ektlari tomonidan o‘z aktivlarini himoya qilish maqsadida amalga oshiriladi.

O‘zbekiston Respublikasining **"Kiberxavfsizlik to‘g‘risida"gi Qonuni** monitoring jarayonining sub'ektlari va ularning huquqiy maqomini belgilab bergan [^1]. Ushbu qonunga ko‘ra, monitoring natijasida olingan ma’lumotlar kiberhodisaga huquqiy baho berishda asosiy manba hisoblanadi.

O‘zbekistonda monitoring tizimi quyidagi iyerarxik tuzilmaga asoslanadi:

- **Konstitutsiyaviy normalar:** Axborot olish va uni himoya qilish huquqi.
- **Qonunlar:** "Kiberxavfsizlik to‘g‘risida", "Axborotlashtirish to‘g‘risida", "Shaxsga doir ma’lumotlar to‘g‘risida".
- **Prezident farmon va qarorlari:** Masalan, PQ-4024-sonli qaror kiberxavfsizlikni nazorat qilishning tashkiliy mexanizmlarini belgilaydi [^2].

Huquqiy tartibga solishning o‘ziga xosligi shundaki, monitoring jarayonida to‘planadigan ma’lumotlar (trafik tahlili, loglar) "shaxsiy hayot daxlsizligi" prinsiplari bilan to‘qnash kelishi mumkin. Shu sababli, qonunchilik monitoring sub'ektlariga faqat xavfsizlik maqsadlarida ma’lumot yig‘ish majburiyatini yuklaydi.

Monitoring tizimining markazida **"Kiberxavfsizlik markazi" DUK** va **Davlat xavfsizlik xizmati** turadi. Ularning vakolatlari doirasiga quyidagilar kiradi:

1. Davlat organlari axborot tizimlarining xavfsizligini masofaviy monitoring qilish.
2. Kiberhujumlar aniqlanganda ularni bartaraf etish bo‘yicha ko‘rsatmalar berish.
3. Axborot tizimlarining kiber-auditini o‘tkazish.

Ma’lumotlarga ko‘ra, birgina 2024-2025 yillarda O‘zbekiston milliy segmentidagi davlat resurslariga qilingan hujumlarning 70% dan ortig‘i monitoring tizimlarining tezkorligi tufayli bartaraf etilgan [^3].

Xalqaro tajriba: Qiyosiy-huquqiy tahlil

Monitoring sohasida **Estoniya** va **Isroil** tajribasi diqqatga sazovordir. Estoniyada kiber-monitoring tizimi markazlashgan bo‘lib, davlat va xususiy sektor o‘rtasida real vaqt rejimida ma’lumot almashish (X-Road tizimi orqali) huquqiy jihatdan majburiy qilib qo‘yilgan.

O‘zbekiston uchun ushbu tajribadan quyidagi jihatlarni o‘zlashtirish muhim:

- Kiber-hodisalar haqida xabar bermaslik uchun yuridik javobgarlikni kuchaytirish.
- Monitoring ma’lumotlarini avtomatlashtirilgan holda huquqni muhofaza qiluvchi organlarga uzatish mexanizmini joriy etish.

Monitoring jarayonida shakllanadigan raqamli dalillar (Digital Evidence) jinoyat va ma’muriy ishlar bo‘yicha muhim ahamiyatga ega. **O‘zbekiston Jinoyat-protsessual kodeksi** va **Ma’muriy javobgarlik to‘g‘risidagi kodeksga** kiritilgan so‘nggi o‘zgarishlar kiber-monitoring hisobotlarini sudlarda dalil sifatida ishlatish imkonini beradi [^4].

Tavsiyalar: Tadqiqot natijalariga ko‘ra, sohani yanada takomillashtirish uchun quyidagilar taklif etiladi:

1. **Kiber-sug‘urta institutini joriy etish:** Monitoring tizimini o‘rnatgan tashkilotlar uchun kiber-sug‘urta tariflarini pasaytirish bo‘yicha huquqiy rag‘batlantirish mexanizmini yaratish.
2. **Yagona kiber-monitoring reglamenti:** Barcha vazirlik va idoralar uchun monitoring olib borishning yagona standartlashtirilgan huquqiy tartibini ishlab chiqish.
3. **Kiber-prokuror nazorati:** Monitoring jarayonida inson huquqlari va shaxsiy ma’lumotlar daxlsizligi buzilmasligini nazorat qilish uchun prokuratura tizimida ixtisoslashgan bo‘limlarni kuchaytirish.

Xulosa

Kiberxavflarni monitoring qilishning huquqiy asoslarini mustahkamlash — bu nafaqat texnologik ehtiyoj, balki davlatning raqamli suverenitetini ta’minlashning garovidir. Monitoring tizimi takomillashgani sari, uning huquqiy tartibga solinishi ham mos ravishda inson huquqlari va jamoat xavfsizligi o‘rtasidagi muvozanatni saqlab qolishi lozim.

FOYDALANILGAN MANBALAR:

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni.

2. O‘zbekiston Respublikasi Prezidentining 2018-yil 21-noyabrdagi PQ-4024-sonli qarori.

3. "Kiberxavfsizlik markazi" DUKning 2025-yil yakunlari bo‘yicha tahliliy ma’lumotnomasi.

4. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi (2024-yil tahriri).

5. Rustambayev M.X. Axborot texnologiyalari sohasidagi jinoyatlar tahlili. – Toshkent: TDYU, 2021.