KIBERXAVF TAHLILI VA UNING HUQUQIY AHAMIYATI

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

Annotatsiya: Mazkur maqolada kiberxavfsizlik tushunchasi, kiberxavflarni tahlil qilish usullari va ushbu jarayonning huquqiy jihatlari tadqiq etiladi. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni doirasida kiberjinoyatchilikka qarshi kurashishning huquqiy asoslari va axborot tizimlarini himoya qilishda risk-tahlilning o'rni yoritilgan.

Kalit so'zlar: kiberxavfsizlik, kiberxavf tahlili, kiberjinoyatchilik, raqamli huquq, axborot infratuzilmasi, risklarni baholash, O'zbekiston qonunchiligi.

Аннотация: В данной статье рассматривается концепция кибербезопасности, методы анализа киберрисков и правовые аспекты этого процесса. Освещена правовая база борьбы с киберпреступностью и роль анализа рисков в защите информационных систем в рамках Закона Республики Узбекистан «О кибербезопасности».

Ключевыеслова: кибербезопасность, анализ киберрисков, киберпреступность, цифровое право, информационная инфраструктура, оценка рисков, узбекское законодательство.

Abstract: This article examines the concept of cybersecurity, methods of analyzing cyber risks, and the legal aspects of this process. The legal framework for combating cybercrime and the role of risk analysis in protecting information systems within the framework of the Law of the Republic of Uzbekistan "On Cybersecurity" are highlighted.

Keywords: cybersecurity, cyber risk analysis, cybercrime, digital law, information infrastructure, risk assessment, Uzbek legislation.

Kirish

Bugungi kunda davlat boshqaruvi, iqtisodiyot va ijtimoiy sohalarning raqamli platformalarga o'tishi axborot xavfsizligini ta'minlash masalasini milliy xavfsizlikning ajralmas qismiga aylantirdi. Kiberxavf — bu axborot tizimlari, resurslari va ma'lumotlariga nisbatan amalga oshirilishi mumkin bo'lgan tahdidlarning ehtimollik darajasidir. Kiberxavf tahlili nafaqat texnik choralar, balki huquqiy tartibga solish mexanizmlari bilan ham chambarchas bog'liq.

1. Kiberxavf tahlilining tushunchasi va mohiyati

Kiberxavf tahlili (Cyber Risk Assessment) — bu tizimdagi zaifliklarni aniqlash, potentsial tahdidlarni baholash va ularning oqibatlarini minimallashtirish jarayonidir. O'zbekiston Respublikasining **"Kiberxavfsizlik to'g'risida"gi Qonuni**ning 3-moddasida kiberxavfsizlikka "kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati" deya ta'rif berilgan [^1].

Kiberxavf tahlili quyidagi bosqichlarni o‘z ichiga oladi:

- **Aktivlarni identifikatsiya qilish:** Himoya qilinishi kerak bo‘lgan ma’lumotlar va infratuzilmani aniqlash.
- **Tahdidlarni baholash:** Tashqi (xakerlik hujumlari, viruslar) va ichki (xodimlarning xatosi, ma’lumotlar sizib chiqishi) xavflarni tahlil qilish.
- **Oqibatlarni prognozlash:** Kiberhujum natijasida ko‘rilishi mumkin bo‘lgan moddiy va ma’naviy zararni hisoblash.

2. Kiberxavf tahlilining huquqiy ahamiyati

Kiberxavflarni tahlil qilish huquqiy nuqtai nazardan bir necha muhim funksiyalarni bajaradi:

A. Javobgarlikni belgilash: Huquqiy amaliyotda "lozim darajadagi ehtiyotkorlik" (due diligence) prinsipi mavjud. Agar tashkilot kiberxavf tahlilini o‘z vaqtida o‘tkazmagan bo‘lsa va buning natijasida shaxsga doir ma’lumotlar o‘g‘irlansa, ushbu holat tashkilotning huquqiy javobgarligini og‘irlashtiruvchi omil bo‘lib xizmat qiladi [^2].

B. Muhim axborot infratuzilmasi ob'ektlarini himoya qilish: O‘zbekiston qonunchiligiga ko‘ra, muhim axborot infratuzilmasi (MAI) ob'ektlari egalari muntazam ravishda kiberxavfsizlik auditidan o‘tishlari shart. Bu kiberxavf tahlilining majburiy huquqiy talab ekanligini ko‘rsatadi [^3].

V. Dalillar bazasini yaratish: Kiberhujum sodir bo‘lganda, avvaldan o‘tkazilgan tahlil hisobotlari sud jarayonida kiberjinoyatning qanday sharoitda va qaysi zaiflik orqali sodir etilganini isbotlash uchun asosiy dalil bo‘lib xizmat qilishi mumkin.

3. O‘zbekiston qonunchiligida kiberxavfsizlik masalalari

O‘zbekiston Respublikasi Jinoyat kodeksining XX¹ bobi ("Axborot texnologiyalari sohasidagi jinoyatlar") kiberjinoyatlar uchun jinoiy javobgarlikni belgilaydi. Biroq, kiberxavf tahlili ko‘proq **preventiv (oldini oluvchi)** ahamiyatga ega.

"Kiberxavfsizlik sohasidagi huquqbuzarliklarning oldini olish, kiberxavf tahlilining samaradorligiga bevosita bog‘liq. Zero, huquqiy norma faqat jinoyat sodir etilgandan keyin jazo berishni emas, balki uning oldini olish choralarini ham tartibga solishi lozim" [^4].

Xulosa

Kiberxavf tahlili shunchaki IT-mutaxassislarining vazifasi emas, balki tashkilotning huquqiy xavfsizligini ta’minlovchi strategik vositadir. Tizimli tahlil orqali:

1. Kiberjinoyatlarning huquqiy oqibatlari kamaytiriladi;
2. Shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilik talablari bajariladi;
3. Davlatning kiber-mudofaa qobiliyati mustahkamlanadi.

Kelajakda O‘zbekiston qonunchiligiga kiberxavflarni majburiy sug‘urtalash (Cyber Insurance) mexanizmlarini kiritish va bu jarayonda risk-tahlil hisobotlarini huquqiy hujjat sifatida tan olish maqsadga muvofiqdir.

Foydalanilgan manbalar:

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni. O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi.

2. Gulyamov S.S. Raqamli huquq: Darslik. – Toshkent: TDYU, 2023. – B. 145-148.

3. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 12-oktabrdagi "Kiberxavfsizlik sohasidagi ayrim normativ-huquqiy hujjatlarni tasdiqlash to‘g‘risida"gi 588-son qarori.

4. Rustambayev M.X. O‘zbekiston Respublikasi Jinoyat huquqi kursi. Maxsus qism. – Toshkent: Sharq, 2021. – B. 512.

5. "Kiberxavfsizlik markazi" DUK rasmiy tahliliy hisobotlari (uzcert.uz).