

ELEKTRON XAVFSIZLIK

Ismanova Marg'uba Numonovna

IIV Namangan akademik litsey Informatika va AT fani o'qituvchisi

marguba0103@gmail.com

Annotatsiya.

Maqolada elektron xavfsizlik, axborot xavfsizligi va kiberxavfsizlik sohalarining raqamli transformatsiya jarayonidagi roli keng yoritilgan. Kiberxavf-xatarlarning ko'payishi, ayniqsa ijtimoiy ahamiyatga ega infratuzilmalarga nisbatan tahdidlarning kuchaygani tahlil qilingan. Axborot xavfsizligiga tizimli yondashuv — texnik, tashkiliy, huquqiy va inson omillarining uyg'unligi asosida muhokama etilgan. Shuningdek, milliy qonunchilik va xalqaro standartlar o'rtasidagi integratsiya masalasi ham ko'rib chiqilgan. Shu bilan bir qatorda, texnologik, huquqiy va madaniy yondashuvlarni uyg'unlashtirish orqali O'zbekistonda samarali elektron xavfsizlik tizimini barpo etish mumkinligi asoslab berilgan.

Kalit so'zlar Elektron xavfsizlik, axborot xavfsizligi, kiberxavfsizlik, raqamli transformatsiya, kiberxavf-xatarlar, tizimli yondashuv, normativ-huquqiy baza, xavfsizlik madaniyati

ЭЛЕКТРОННАЯ БЕЗОПАСНОСТЬ

Исманова Маргуба Нумановна

Преподаватель информатики и информационных технологий

Академического лицея МВД, г. Наманган

marguba0103@gmail.com

Аннотация: В статье широко освещена роль электронной безопасности, информационной безопасности и кибербезопасности в процессе цифровой трансформации. Проанализировано увеличение числа киберугроз, особенно в отношении социально значимой инфраструктуры. Информационная безопасность рассматривается с системной точки зрения — на основе взаимодействия технических, организационных, правовых и человеческих факторов. Также рассмотрены вопросы интеграции между национальным законодательством и международными стандартами. Кроме того, в исследовании обоснована возможность построения эффективной системы

электронной безопасности в Узбекистане за счёт объединения технологических, правовых и культурных подходов.

Ключевые слова: Электронная безопасность, информационная безопасность, кибербезопасность, цифровая трансформация, киберугрозы, системный подход, нормативно-правовая база, культура безопасности.

ELECTRONIC SECURITY

Ismanova Marguba Numonovna

Teacher of Informatics and Information Technologies

Academic Lyceum of the Ministry of Internal Affairs, Namangan

marguba0103@gmail.com

Abstract: The article provides a comprehensive overview of the role of electronic security, information security, and cybersecurity in the process of digital transformation. It analyzes the growing number of cyber threats, particularly those targeting socially significant infrastructures. A systematic approach to information security is discussed, emphasizing the integration of technical, organizational, legal, and human factors. The study also addresses the issue of aligning national legislation with international standards. Furthermore, it substantiates that by combining technological, legal, and cultural approaches, it is possible to establish an effective electronic security system in Uzbekistan.

Keywords: Electronic security, information security, cybersecurity, digital transformation, cyber threats, systematic approach, regulatory framework, security culture

KIRISH

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi insoniyat hayotining barcha jabhalariga, xususan, ijtimoiy, iqtisodiy va ilmiy sohalarga chuqur kirib bordi. Bugungi kunda elektron qurilmalar, tarmoqlar va raqamli axborot resurslari faoliyatimizning ajralmas qismiga aylangan bo'lsa-da, ularning xavfsizligi masalasi global miqyosda dolzarb muammoga aylanmoqda. Ayniqsa, raqamli transformatsiya jarayonlarining kengayib borishi bilan birga,

kiberhujumlar, ma'lumotlarni noqonuniy egallash, tizimlarga ruqsatsiz kirish kabi xavf-xatarlar ham ortib bormoqda.

Elektron xavfsizlik — bu nafaqat texnik masala, balki iqtisodiy, siyosiy va huquqiy jihatlariga ega bo'lgan ko'p qirrali sohadir. Ushbu sohaning asosiy vazifasi — axborot resurslarini har qanday tahdid va hujumlardan himoya qilish, foydalanuvchilar shaxsiy ma'lumotlari, moliyaviy va intellektual mulk xavfsizligini ta'minlashdan iborat. Elektron xavfsizlik siyosatining izchil va samarali yuritilishi zamonaviy raqamli davlat barpo etish yo'lida muhim ahamiyat kasb etadi.

Mazkur maqolada elektron xavfsizlik sohasining dolzarb muammolari, mavjud tahdidlar, himoya strategiyalari hamda ushbu sohada ilg'or texnologiyalarni joriy etishning ilmiy-nazariy asoslari tahlil qilinadi. Shu bilan birga, milliy va xalqaro tajribalar asosida elektron xavfsizlikni ta'minlashda qo'llanilayotgan usullarning samaradorligi baholanadi va istiqboldagi rivojlanish yo'nalishlari yuzasidan ilmiy xulosalar keltiriladi.

ADABIYOTLAR TAHLILI VA METODOLOGIYASI

Elektron xavfsizlik, axborot xavfsizligi va kiberxavfsizlik bugungi kunda butun dunyo miqyosida eng dolzarb muammolardan biri sifatida qaralmoqda. Raqamli texnologiyalarning jadal rivojlanishi va internet infratuzilmasining kengayib borishi bilan bu yo'nalishlarda olib borilayotgan ilmiy tadqiqotlar soni keskin oshdi. Mazkur sohalar nafaqat texnik aspektlarni, balki iqtisodiy, huquqiy va ijtimoiy jihatlarni ham o'z ichiga oladi. Shu sababli, mavjud ilmiy manbalarni tahlil qilish orqali ushbu yo'nalishlardagi dolzarb muammolarni aniqlash va ularni hal etish mexanizmlarini chuqur o'rganish zarur.

Axborot xavfsizligi va elektron xavfsizlikning texnik asoslari ilk bor Anderson tomonidan taqdim etilgan bo'lib, u o'zining "Security Engineering" nomli fundamental asarida tizim xavfsizligini ta'minlashda shifrlash algoritmlari, autentifikatsiya, tarmoq xavfsizligi hamda ma'lumotlarni saqlash muhimligini ta'kidlaydi. Andersonning fikricha, har bir xavfsizlik tizimi komponenti xavf-xatarlarni minimallashtirish maqsadida puxta ishlab chiqilishi lozim. U xavfsizlikni inson omili, tizim va protseduralar o'rtasidagi o'zaro bog'liqlik nuqtayi nazaridan ham tahlil qiladi [1].

O'zbekistonlik tadqiqotchilar ham ushbu yo'nalishda faol ilmiy izlanishlar olib bormoqdalar. Xususan, A.Shavkatov o'zining "Axborot xavfsizligi va uning ta'minlanishida milliy standartlar" nomli tadqiqotida axborot xavfsizligi sohasidagi milliy yondashuvlar va xalqaro tajribalarni atroflicha tahlil qilgan bo'lib, axborot xavfsizligiga oid normativ-huquqiy bazani takomillashtirish zaruratini asoslab beradi [2].

I.Rasulov tomonidan yozilgan "Axborot xavfsizligini ta'minlashda tizimli yondashuv" asarida esa axborot xavfsizligini boshqarish, infratuzilmani himoya qilish va xavf-xatarlarni baholash tizimlari chuqur tahlil qilinadi. Muallifning ta'kidlashicha, xavfsizlikni ta'minlash faqat texnologik yechimlar bilan emas, balki tashkiliy va psixologik yondashuvlar bilan uyg'un holda amalga oshirilishi lozim [3].

Shuningdek, M.Mustafayev tomonidan e'lon qilingan "Kiberxavfsizlik va uning asosiy tamoyillari" nomli o'quv qo'llanma zamonaviy kiberxavf-xatarlar, ularga qarshi kurashish strategiyalari va kiberxavfsizlik siyosatining huquqiy asoslarini qamrab olgan. Ushbu asarda axborot muhofazasi, tarmoq xavfsizligi hamda foydalanuvchilarning shaxsiy ma'lumotlarini himoyalashga doir uslublar atroflicha yoritilgan [4].

Bundan tashqari, O'zbekiston Respublikasining "Axborot xavfsizligi to'g'risida"gi Qonuni, "Elektron hukumat to'g'risida"gi Qonuni, shuningdek, Prezident farmonlari va Vazirlar Mahkamasi qarorlari elektron xavfsizlik siyosatini amaliyotda joriy qilishda muhim huquqiy asos bo'lib xizmat qilmoqda [5][6].

MUHOKAMA VA NATIJALAR

Bugungi kunda elektron xavfsizlik, axborot xavfsizligi va kiberxavfsizlik sohalarida raqamli transformatsiya jarayonining ajralmas qismiga aylangan. Bu jarayon nafaqat texnik vositalarni, balki inson omili, huquqiy asoslar va tashkiliy tuzilmalarning hamkorlikda faoliyat yuritishini talab qiladi.

Kiberxavf-xatarlarning ko'payishi va murakkablashuvi — Raqamli texnologiyalar hayotimizning barcha sohalariga chuqur kirib kelgan bir paytda, kiberhujumlar soni ham ortib bormoqda. Ayniqsa, bank tizimlari, elektron hukumat, ta'lim, sog'liqni saqlash kabi ijtimoiy muhim infratuzilmalarga nisbatan

yo‘naltirilgan hujumlar xavfi kuchaygan. Bu esa himoya tizimlarini yangilab borishni taqozo etadi.

Axborot xavfsizligiga tizimli yondashuvning dolzarbligi — Axborot xavfsizligini ta‘minlashda faqat texnik choralar bilan cheklanib qolmasdan, foydalanuvchi xulq-atvori, tashkiliy siyosatlar, xavfsizlik madaniyati, hamda normativ-huquqiy mexanizmlar uyg‘unligini ta‘minlash zarur.

Milliy qonunchilik va xalqaro tajriba uyg‘unligini ta‘minlash — O‘zbekiston Respublikasining “Axborot xavfsizligi to‘g‘risida”gi Qonuni va unga doir normativ-huquqiy hujjatlar mavjud bo‘lsa-da, xalqaro standartlar (masalan, ISO/IEC 27001) bilan moslik darajasi doimiy tahlil etilishi va yangilanib borilishi kerak. Shuningdek, xalqaro hamkorlikni kengaytirish orqali eng yaxshi tajribalarni amaliyotga joriy etish muhim sanaladi.

Axborot xavfsizligi madaniyatini shakllantirish — Tadqiqot jarayonida axborot xavfsizligini faqat mutaxassislar emas, balki oddiy foydalanuvchilar darajasida ham tushunish va unga amal qilish zarurligi o‘z isbotini topdi. Shu sababli, ta‘lim muassasalarida axborot xavfsizligiga oid bilimlarni erta bosqichdanoq berish, ommaviy axborot vositalarida bu borada targ‘ibot ishlarini kuchaytirish dolzarbdir.

Bugungi kunda axborot va kiberxavfsizlik sohasida samarali boshqaruv, zamonaviy texnologiyalarni tatbiq etish, huquqiy asoslarni takomillashtirish, hamda foydalanuvchilarda xavfsizlik madaniyatini shakllantirish asosiy yo‘nalishlar sifatida ajralib turadi. Tadqiqot natijalari shuni ko‘rsatdiki, ushbu yondashuvlarni uyg‘unlashtirish orqali O‘zbekistonda elektron xavfsizlik tizimini zamon talablari darajasida tashkil etish mumkin.

XULOSA

Axborot xavfsizligini ta‘minlashda texnik himoya vositalari bilan bir qatorda huquqiy me‘yorlar, tashkiliy chora-tadbirlar, foydalanuvchilar bilim darajasini oshirish va xavfsizlik madaniyatini shakllantirish muhim omillar hisoblanadi.

O‘zbekiston Respublikasida ham axborot xavfsizligiga oid normativ-huquqiy baza shakllantirilgan va izchil takomillashtirib borilmoqda. Biroq amaliyotda yuzaga kelayotgan yangi xavf-xatarlar, ayniqsa kiberhujumlar, bu tizimni yanada mustahkamlash va ilg‘or tajribalarni joriy qilish zarurligini ko‘rsatmoqda.

Shu asosda, quyidagilarga ko'proq e'tibor qaratilishi taqazo etiladi :

- Elektron xavfsizlikni ta'minlash – bu faqat IT sohasining vazifasi emas, balki davlat, biznes va fuqarolik jamiyati vakillarining hamkorligini talab qiladigan umumjamoaviy masaladir;
- Axborot xavfsizligini mustahkamlashda raqamli savodxonlikni oshirish va xavfsizlik madaniyatini shakllantirish dolzarb ahamiyat kasb etadi;
- Mavjud qonunchilik xalqaro standartlarga uyg'unlashtirilib, ularning amaliyotga tatbiq etilishini nazorat qilish zarur;

Tashkilotlar miqyosida axborot xavfsizligi siyosatlarini ishlab chiqish, xavf-xatarlarni baholash hamda ularning oldini olishga yo'naltirilgan doimiy monitoring tizimini yo'lga qo'yish muhim ahamiyat kasb etadi. Umuman olganda, elektron xavfsizlikni ta'minlash – bu zamon talabi bo'lib, u har bir davlatning axborot suverenitetini, iqtisodiy barqarorligini va fuqarolar huquqlarini himoya qilishda asosiy omillardan biridir.

Foydalanilgan adabiyotlar ro'yxati

1. R.Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley-2021.
2. A.Shavkatov. Axborot xavfsizligi va uning ta'minlanishida milliy standartlar. Toshkent: Innovatsion nashriyot-2021.
3. I.Rasulov. Axborot xavfsizligini ta'minlashda tizimli yondashuv. Toshkent: Fan va texnologiya-2022.
4. M.Mustafayev. Kiberxavfsizlik va uning asosiy tamoyillari. Toshkent: Axborot xavfsizligi markazi nashriyoti-2023.
5. O'zbekiston Respublikasi "Axborot xavfsizligi to'g'risida"gi Qonuni. 2020-yil.
6. O'zbekiston Respublikasi "Elektron hukumat to'g'risida"gi Qonuni. 2015-yil.
7. O'zbekiston Respublikasi Prezidenti Sh.M. Mirziyoyev. "Raqamli O'zbekiston – 2030" strategiyasi va uning amalga oshirilishiga oid qaror va farmonlar. Toshkent-2020.