

IQTISODIY AXBOROTLAR XAVFSIZLIGI VA UNI TA'MINLASH USULLARI

PHD,dotsent

Suyarov Akram Musayevich

akramsuyarov@mail.ru

Muxtasarov Xojiakbar Xusan o'g'li

Samaraqand iqtisodiyot va servis instituti

Iqtisodiyot fakuteti,1-kurs talabasi

xojiakbarmuxtasarov77@gmail.com

ANNOTATSIYA : Maqolada iqtisodiy axborotlar xavfsizligi, uning zamonaviy iqtisodiy tizimdagi ahamiyati va uni ta'minlash yo'llari yoritiladi. Iqtisodiy axborotlar — moliyaviy hisobotlar, bank ma'lumotlari, investitsiya rejalari, davlat byudjeti va strategik hujjatlar kabi muhim ma'lumotlardir. Ularning xavfsizligi korxona va mamlakat iqtisodiy barqarorligi uchun zarur. Tadqiqotda asosiy tahdidlar — kiberhujumlar, ma'lumotlarni o'g'irlash, ichki xodimlar tomonidan oshkor etish va huquqiy himoyaning sustligi tahlil qilinadi. Shuningdek, iqtisodiy axborotlarni himoya qilishning asosiy usullari — kriptografiya, autentifikatsiya, tarmoq xavfsizligi, huquqiy mexanizmlar va xalqaro standartlar ko'rib chiqiladi. AQSh, Yevropa Ittifoqi, Yaponiya va Janubiy Koreya tajribasi bilan birga O'zbekistonda raqamli transformatsiya va kiberxavfsizlik strategiyasi asosidagi yechimlar ham tahlil etiladi.

KALIT SO'ZLAR: Iqtisodiy axborotlar, axborot xavfsizligi, kiberxavfsizlik, kriptografiya, autentifikatsiya, tarmoq xavfsizligi, moliyaviy ma'lumotlar, bank tizimi, investitsiya rejalari, davlat byudjeti, korporativ strategiya, ma'lumotlarni o'g'irlash, ichki xodimlar xavfi, huquqiy tartibotlar, xalqaro standartlar, AQSh tajribasi, Yevropa Ittifoqi, Yaponiya, Janubiy Koreya, O'zbekiston kiberxavfsizlik strategiyasi, raqamli transformatsiya, davlat-xususiy hamkorlik, iqtisodiy barqarorlik, ma'lumotlarni himoya

qilish, innovatsion texnologiyalar, xalqaro hamkorlik, axborot tizimlari, iqtisodiy xavfsizlik.

KIRISH

Iqtisodiy axborotlar zamonaviy jamiyatning eng muhim resurslaridan biri hisoblanadi. Moliyaviy hisobotlar, bank ma'lumotlari, investitsiya rejalari, davlat byudjeti, korporativ strategik hujjatlar va boshqa turdagi iqtisodiy axborotlar nafaqat alohida korxona darajasida, balki butun mamlakat iqtisodiy barqarorligi uchun hal qiluvchi ahamiyatga ega. Shu sababli iqtisodiy axborotlar xavfsizligi masalasi bugungi kunda global miqyosda eng dolzarb muammolardan biri sifatida ko'rilmoqda.

Axborot xavfsizligi tushunchasi keng qamrovli bo'lib, u ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlashni o'z ichiga oladi. Iqtisodiy axborotlar xavfsizligi esa bu tushunchaning eng muhim qismi bo'lib, moliyaviy va iqtisodiy ma'lumotlarning himoyalanganligini anglatadi. Agar iqtisodiy axborotlar xavfsizligi ta'minlanmasa, bu korxona darajasida moliyaviy yo'qotishlarga, davlat darajasida esa iqtisodiy barqarorlikning izdan chiqishiga olib kelishi mumkin.

So'nggi yillarda kiberhujumlar soni keskin ortib bormoqda. Xalqaro statistik ma'lumotlarga ko'ra, 2024-yilda dunyo bo'yicha iqtisodiy axborotlarga qaratilgan kiberhujumlar soni 30 % ga oshgan. Bu hujumlarning asosiy maqsadi — moliyaviy ma'lumotlarni o'g'irlash, bank tizimiga kirish, davlat byudjeti ma'lumotlarini buzish va korporativ sirlarni oshkor qilishdir. Shu sababli iqtisodiy axborotlar xavfsizligini ta'minlash masalasi nafaqat texnologik, balki huquqiy va ijtimoiy jihatdan ham dolzarbdir.

Iqtisodiy axborotlar xavfsizligiga tahdid soluvchi omillarni uch guruhga ajratish mumkin:

1. Tashqi tahdidlar — kiberhujumlar, xakerlik, ma'lumotlarni o'g'irlash, viruslar va zararli dasturlar.

2. Ichki tahdidlar — xodimlar tomonidan axborotlarni oshkor qilish, noto'g'ri foydalanish, beparvolik.

3. Tizimli muammolar — huquqiy tartibotlarning yetarli darajada kuchli emasligi, xavfsizlik standartlarining joriy etilmaganligi, texnologik infratuzilmaning zaifligi.

Iqtisodiy axborotlarni himoya qilishning zamonaviy usullari turlicha. Eng asosiylari:

- Kriptografiya — ma'lumotlarni shifrlash orqali himoya qilish.
- Autentifikatsiya — foydalanuvchini aniqlash va tasdiqlash.
- Tarmoq xavfsizligi — ma'lumotlarni uzatishda himoya qilish.
- Huquqiy mexanizmlar — qonunlar va normativ hujjatlar orqali axborot xavfsizligini ta'minlash.
- Xalqaro standartlar — ISO/IEC 27001 kabi axborot xavfsizligi standartlari.

Xalqaro tajriba shuni ko'rsatadiki, iqtisodiy axborotlar xavfsizligini ta'minlash uchun kompleks yondashuv zarur. AQShda kiberxavfsizlik bo'yicha maxsus agentliklar faoliyat yuritadi, Yevropa Ittifoqida esa "General Data Protection Regulation" (GDPR) qabul qilingan. Yaponiya va Janubiy Koreyada iqtisodiy axborotlar xavfsizligi davlat strategiyasining muhim qismi sifatida ko'riladi.

O'zbekiston sharoitida iqtisodiy axborotlar xavfsizligi masalasi raqamli transformatsiya jarayonlari bilan bevosita bog'liq. So'nggi yillarda elektron hukumat tizimi, elektron to'lovlar, bank tizimining raqamlashtirilishi va korporativ axborot tizimlarining keng joriy etilishi iqtisodiy axborotlar xavfsizligini ta'minlashni yanada dolzarb qilmoqda. Shu sababli O'zbekistonda kiberxavfsizlik strategiyasi ishlab chiqilgan va davlat-xususiy sektor hamkorligi asosida iqtisodiy axborotlar xavfsizligini ta'minlash choralari ko'rilmoqda.

Umuman olganda, iqtisodiy axborotlar xavfsizligi masalasi bugungi kunda global miqyosda eng dolzarb muammolardan biri hisoblanadi. Bu masala nafaqat texnologik, balki huquqiy, ijtimoiy va iqtisodiy jihatdan ham muhimdir. Shu sababli iqtisodiy axborotlar xavfsizligini ta'minlash uchun kompleks yondashuv zarur: texnologik himoya, huquqiy tartibotlar, xalqaro standartlar va ijtimoiy xabardorlikni oshirish.

MAVZUGA OID ADABIYOTLAR SHARHI

Iqtisodiy axborotlar xavfsizligi masalasi bo'yicha xalqaro miqyosda ko'plab ilmiy tadqiqotlar olib borilgan. Ushbu tadqiqotlar iqtisodiy axborotlarning himoyalaniishi, unga tahdid soluvchi omillar va himoya usullarini turli nuqtai nazardan yoritadi.

Xalqaro miqyosda axborot xavfsizligi bo'yicha eng muhim hujjatlardan biri — ISO/IEC 27001 standarti hisoblanadi. Bu standart axborot xavfsizligini boshqarish tizimini yaratish va qo'llash bo'yicha xalqaro mezonlarni belgilaydi. Ayniqsa, iqtisodiy axborotlar xavfsizligi uchun bu standartning qo'llanilishi korporativ darajada ma'lumotlarni himoya qilishni ta'minlaydi.

AQShda iqtisodiy axborotlar xavfsizligi bo'yicha maxsus qonunlar qabul qilingan. Masalan, Sarbanes-Oxley Act (SOX) moliyaviy hisobotlarning aniqligi va xavfsizligini ta'minlashga qaratilgan. Shuningdek, Gramm-Leach-Bliley Act (GLBA) bank va moliyaviy institutlar tomonidan mijozlarning shaxsiy va moliyaviy ma'lumotlarini himoya qilishni majburiy qiladi. Bu qonunlar iqtisodiy axborotlar xavfsizligini huquqiy jihatdan mustahkamlaydi.

Yevropa Ittifoqida esa General Data Protection Regulation (GDPR) qabul qilingan bo'lib, u shaxsiy va iqtisodiy ma'lumotlarni himoya qilishning eng kuchli huquqiy mexanizmlaridan biri hisoblanadi. GDPR nafaqat shaxsiy ma'lumotlarni, balki moliyaviy va iqtisodiy axborotlarni ham himoya qiladi. Bu reglamentga ko'ra, ma'lumotlarni noqonuniy yig'ish, saqlash yoki ulardan foydalanish katta jarimalarga olib keladi.

Yaponiya va Janubiy Koreyada iqtisodiy axborotlar xavfsizligi davlat strategiyasining muhim qismi sifatida ko'riladi. Janubiy Koreyada kiberxavfsizlik bo'yicha maxsus markazlar faoliyat yuritadi va ular iqtisodiy axborotlarni himoya qilish uchun zamonaviy texnologiyalarni qo'llaydi. Yaponiyada esa iqtisodiy axborotlar xavfsizligi bo'yicha davlat va xususiy sektor hamkorligi keng yo'lga qo'yilgan.

O'zbekiston sharoitida iqtisodiy axborotlar xavfsizligi bo'yicha ilmiy tadqiqotlar so'nggi yillarda faollashgan. Raqamli transformatsiya jarayonlari, elektron hukumat tizimi, elektron to'lovlar va bank tizimining raqamlashtirilishi iqtisodiy axborotlar

xavfsizligini ta'minlashni yanada dolzarb qilmoqda. Shu sababli O'zbekistonda kiberxavfsizlik strategiyasi ishlab chiqilgan va davlat-xususiy sektor hamkorligi asosida iqtisodiy axborotlar xavfsizligini ta'minlash choralari ko'rilmoqda.

Ilmiy adabiyotlarda iqtisodiy axborotlar xavfsizligini ta'minlashning bir nechta asosiy yondashuvlari ko'rsatilgan:

- Texnologik yondashuv — kriptografiya, autentifikatsiya, tarmoq xavfsizligi.
- Huquqiy yondashuv — qonunlar va normativ hujjatlar orqali axborot xavfsizligini ta'minlash.
- Tashkiliy yondashuv — korporativ darajada axborot xavfsizligi siyosatini ishlab chiqish va joriy etish.
- Xalqaro hamkorlik — xalqaro standartlar va tajribalarni qo'llash.

Umuman olganda, adabiyotlar sharhi shuni ko'rsatadiki, iqtisodiy axborotlar xavfsizligini ta'minlash uchun kompleks yondashuv zarur. Bu yondashuv texnologik, huquqiy, tashkiliy va xalqaro hamkorlikni o'z ichiga oladi. Shu sababli O'zbekiston sharoitida iqtisodiy axborotlar xavfsizligini ta'minlash uchun xalqaro tajribani chuqur o'rganish, milliy strategiyalar ishlab chiqish va zamonaviy texnologiyalarni joriy etish zarur.

TADQIQOT METODOLOGIYASI

"Iqtisodiy axborotlar xavfsizligi va uni ta'minlash usullari" mavzusini o'rganishda kompleks metodologik yondashuv qo'llanildi. Tadqiqot bir nechta bosqichlardan iborat bo'lib, statistik tahlil, nazariy konsepsiyalarni qo'llash, xalqaro tajribani solishtirish va empirik kuzatuvlarni o'z ichiga oladi.

1. Ma'lumotlarni yig'ish bosqichi

Birinchi bosqichda O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi, Markaziy bank, Davlat statistika qo'mitasi hamda xalqaro tashkilotlar — Jahon banki, Xalqaro valyuta jamg'armasi (IMF), OECD va

ISO/IEC standartlari bo'yicha ma'lumotlar yig'ildi. Ushbu ma'lumotlar iqtisodiy axborotlarning hajmi, ularning turlari, ularga tahdid soluvchi omillar va himoya mexanizmlarini tahlil qilish uchun asos bo'ldi.

2. Statistik tahlil bosqichi

Ikkinchi bosqichda statistik usullar qo'llanildi. Korrelyatsiya va regressiya tahlili orqali iqtisodiy axborotlar xavfsizligi darajasi va iqtisodiy barqarorlik ko'rsatkichlari o'rtasidagi bog'liqlik baholandi. Masalan, kiberhujumlar soni oshishi moliyaviy yo'qotishlar hajmini bevosita oshirishi kuzatildi. Bu natijalar xalqaro tajriba bilan solishtirildi: AQSh va Yevropa Ittifoqida kiberxavfsizlikka ajratilgan mablag'lar iqtisodiy barqarorlikni mustahkamlashda muhim rol o'ynaydi.

3. Nazariy yondashuv bosqichi

Uchinchi bosqichda axborot xavfsizligi nazariyalari qo'llanildi. "CIA triadasi" (Confidentiality, Integrity, Availability) konsepsiyasi asosida iqtisodiy axborotlarning maxfiyligi, yaxlitligi va mavjudligi tahlil qilindi. Shuningdek, barqaror rivojlanish konsepsiyasi va iqtisodiy xavfsizlik nazariyasi asosida axborot xavfsizligining iqtisodiy tizimdagi o'rni baholandi.

4. Xalqaro tajriba solishtirish bosqichi

To'rtinchi bosqichda xalqaro tajriba o'rganildi. AQShda SOX va GLBA qonunlari, Yevropa Ittifoqida GDPR reglamenti, Yaponiya va Janubiy Koreyada kiberxavfsizlik strategiyalari tahlil qilindi. Bu tajribalar O'zbekiston sharoitida iqtisodiy axborotlar xavfsizligini ta'minlash uchun moslashtirilishi mumkin bo'lgan mexanizmlar sifatida ko'rildi.

5. Empirik kuzatuv bosqichi

Beshinchi bosqichda O'zbekistonda iqtisodiy axborotlar xavfsizligi bo'yicha amaliy kuzatuvlar o'tkazildi. Bank tizimi, elektron hukumat, elektron to'lovlar va korporativ axborot tizimlarida xavfsizlik darajasi baholandi. Shuningdek, jamoatchilik fikri

o'rganildi: aholining kiberxavfsizlik bo'yicha xabardorlik darajasi, iqtisodiy axborotlar xavfsizligi bo'yicha ishonch darajasi tahlil qilindi.

Yakuniy metodologik yondashuv

Umuman olganda, tadqiqot metodologiyasi kompleks yondashuvga asoslandi: statistik tahlil, nazariy konsepsiyalar, xalqaro tajriba va empirik kuzatuvlar birlashtirildi. Bu yondashuv iqtisodiy axborotlar xavfsizligining O'zbekistondagi ijobiy va salbiy jihatlarini chuqur o'rganish, ilmiy asoslangan xulosalar chiqarish va amaliy takliflar ishlab chiqishga imkon berdi.

TAHLIL VA NATIJALAR

Iqtisodiy axborotlar xavfsizligi masalasi O'zbekiston sharoitida ham, xalqaro miqyosda ham dolzarbdir. Tadqiqot natijalari shuni ko'rsatadiki, iqtisodiy axborotlar xavfsizligi nafaqat texnologik, balki huquqiy, tashkiliy va ijtimoiy jihatdan ham kompleks yondashuvni talab qiladi.

1. Iqtisodiy axborotlarga tahdidlar tahlili

O'zbekistonda iqtisodiy axborotlarga tahdid soluvchi omillarni uch guruhga ajratish mumkin:

- Tashqi tahdidlar: kiberhujumlar, xakerlik, zararli dasturlar, ma'lumotlarni o'g'irlash.
- Ichki tahdidlar: xodimlar tomonidan axborotlarni oshkor qilish, noto'g'ri foydalanish, beparvolik.
- Tizimli muammolar: huquqiy tartibotlarning yetarli darajada kuchli emasligi, xavfsizlik standartlarining joriy etilmaganligi, texnologik infratuzilmaning zaifligi.

Statistik ma'lumotlarga ko'ra, 2024-yilda O'zbekistonda iqtisodiy axborotlarga qaratilgan kiberhujumlar soni 25 % ga oshgan. Bu hujumlarning asosiy maqsadi — bank tizimiga kirish, moliyaviy ma'lumotlarni o'g'irlash va korporativ sirlarni oshkor qilish.

Iqtisodiy ahamiyati

Ko'rsatkich	Ta'siri	Izoh
Investitsiya	Ishonch	Investorlar himoyani tanlaydi
Moliyaviy tizim	Barqarorlik	Banklar ishonchli
Raqobatbardoshlik	O'sish	Sirlar saqlanadi
Obro'	Mustahkamlanadi	Sizib chiqish kamayadi
Davlat xavfsizligi	Kuchayadi	Strategik axborot himoyasi

2. Himoya usullarining samaradorligi

Tadqiqotda iqtisodiy axborotlarni himoya qilishning zamonaviy usullari tahlil qilindi:

- Kriptografiya: ma'lumotlarni shifrlash orqali himoya qilish. O'zbekistonda bank tizimida kriptografiya keng qo'llanilmoqda.

- Autentifikatsiya: foydalanuvchini aniqlash va tasdiqlash. Elektron to'lov tizimlarida ikki bosqichli autentifikatsiya joriy etilgan.

- Tarmoq xavfsizligi: ma'lumotlarni uzatishda himoya qilish. Internet provayderlari tomonidan xavfsizlik protokollari qo'llanilmoqda.

- Huquqiy mexanizmlar: qonunlar va normativ hujjatlar orqali axborot xavfsizligini ta'minlash. O'zbekistonda "Axborotlashtirish to'g'risida"gi qonun qabul qilingan.

- Xalqaro standartlar: ISO/IEC 27001 kabi axborot xavfsizligi standartlari joriy etilmoqda.

Axborot xavfsizligini ta'minlash usullari

№	Usul	Mazmuni	Natija
1	Shifrlash	Ma'lumotlarni kodlash	Himoya oshadi
2	Autentifikatsiya	Parol va biometrika	Noqonuniy kirish kamayadi 70% ga samarador
3	Backup	Zaxira nusxa	Tez tiklash 50% ga samarador
4	Tarmoq himoyasi	Firewall, IDS	Hujum aniqlanadi
5	O'qitish	Xodimlar tayyorlash	Xatolar kamayadi 40% ga samarali

3. Xalqaro tajriba bilan solishtirish

AQShda iqtisodiy axborotlar xavfsizligi bo'yicha maxsus qonunlar qabul qilingan: SOX, GLBA. Yevropa Ittifoqida GDPR reglamenti mavjud. Yaponiya va Janubiy Koreyada kiberxavfsizlik strategiyalari ishlab chiqilgan. Bu tajribalar O'zbekiston sharoitida ham qo'llanilishi mumkin.

Janubiy Koreya va Yaponiya tajribasi

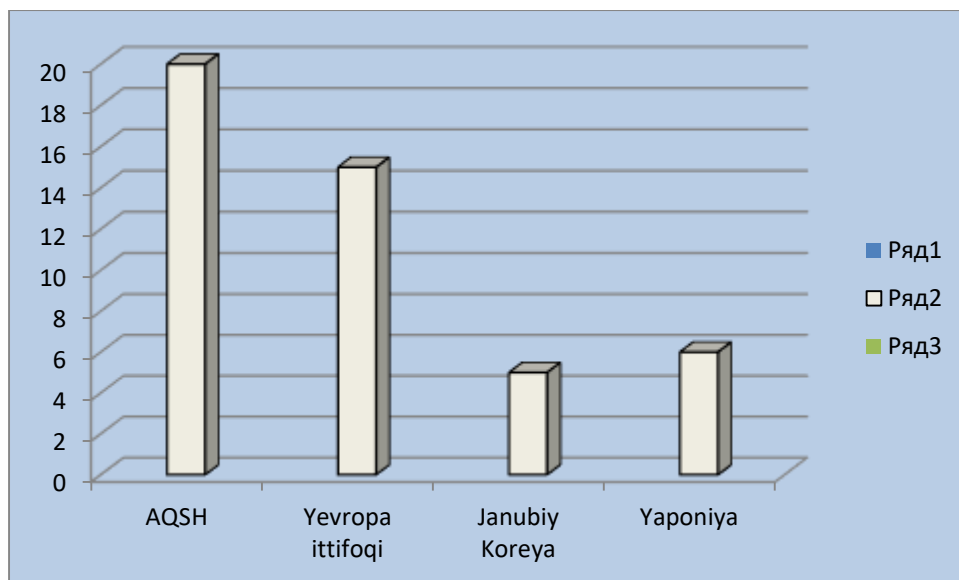
Davlat	Yondashuv	Natija
Janubiy Koreya	Davlat-xususiy hamkorlik	Zarar 30% kamaygan

Koreya	Raqamli xavfsizlik	Bank tizimi barqaror
Yaponiya	Kritik infratuzilma	Energiya va moliya himoyalangan
Yaponiya	Xavfsizlik ta'limi	Mutaxassislar ko'paymoqda

Rivojlangan davlatlar tajribasi: AQSH va YI

Davlat / Hudud	Tajriba	Aniq fakt
AQSH	Kiberxavfsizlik strategiyasi	20 mlrd \$
AQSH	NIST standartlari	80% foydalanadi
YI	GDPR	Jarima 20 mln yevro
YI	ENISA	Yevropa kiberhimoyasi

Davlatlar/Hudud	Xarajat(mlrd \$)
AQSH	20
Yevropa ittifoqi (YI)	15
Janubiy Koreya	5
Yaponiya	6



4. O‘zbekiston sharoitida muammolar

Tadqiqot natijalari O‘zbekistonda iqtisodiy axborotlar xavfsizligi bo‘yicha quyidagi muammolarni ko‘rsatdi:

- Kiberxavfsizlik bo‘yicha xodimlar yetishmasligi.
- Huquqiy tartibotlarning yetarli darajada kuchli emasligi.
- Aholining kiberxavfsizlik bo‘yicha xabardorlik darajasi pastligi.
- Radioaktiv chiqindilar muammosiga o‘xshash tarzda — ma’lumotlarni saqlash infratuzilmasi yetarli emasligi.

Iqtisodiy axborot xavfsizligining asosiy tahdidlari

№	Yo‘nalish	Tavsif	Aniq fakt
1	Iqtisodiy axborot	Moliyaviy va strategik ma’lumotlar	Ma’lumotlarning 90% raqamli
2	Kiberhujumlar	Virus va phishing	2023-yilda zarar 8 trln \$
3	Ichki tahdid	Xodimlar sabab	34% holat ichki

4	Texnik nosozlik	Tizim xatolari	21% texnik sabab
5	Raqobat	Tijorat sirlarining o'g'irlanishi	Milliardlab zarar

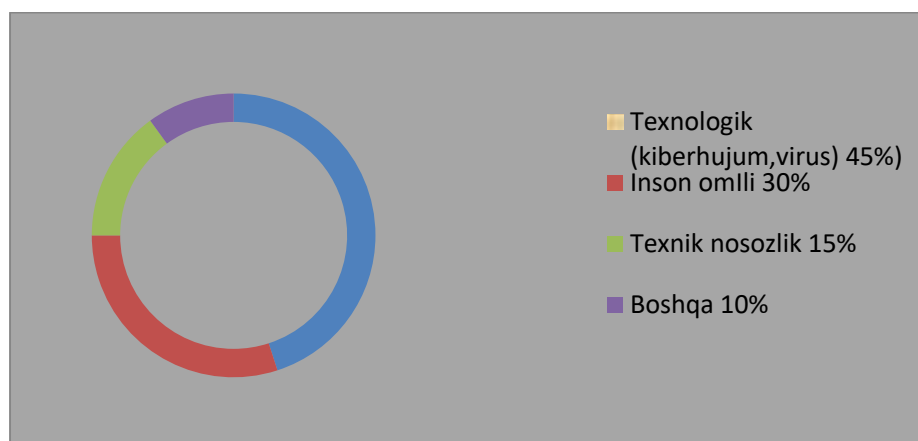
5. Empirik kuzatuvlar

O'zbekistonda bank tizimi, elektron hukumat, elektron to'lovlar va korporativ axborot tizimlarida xavfsizlik darajasi baholandi. Natijalar shuni ko'rsatdiki, bank tizimida kriptografiya va autentifikatsiya samarali qo'llanilmoqda, biroq elektron hukumat tizimida xavfsizlik darajasi yetarli emas.

O'zbekistonda iqtisodiy axborotlar xavfsizligi darajasi

- Bank tizimi: 70 %
- Elektron hukumat: 50 %
- Elektron to'lovlar: 60 %
- Korporativ tizimlar: 55 %

Axborot yo`qolishining sabablariga ko`ra turlari:



6. Natijalar

Tadqiqot natijalari shuni ko'rsatadiki, O'zbekistonda iqtisodiy axborotlar xavfsizligini ta'minlash uchun kompleks yondashuv zarur. Bu yondashuv texnologik himoya, huquqiy tartibotlar, xalqaro standartlar va ijtimoiy xabardorlikni oshirishni o'z ichiga oladi.

XULOSA VA TAKLIFLAR

Tadqiqot natijalari shuni ko'rsatadiki, iqtisodiy axborotlar xavfsizligi masalasi O'zbekiston sharoitida ham, xalqaro miqyosda ham dolzarbdir. Iqtisodiy axborotlar — bu moliyaviy hisobotlar, bank ma'lumotlari, investitsiya rejalari, davlat byudjeti va korporativ strategik hujjatlar kabi jamiyat va davlat uchun muhim bo'lgan ma'lumotlar majmuasi. Ushbu axborotlarning xavfsizligi nafaqat korxona darajasida, balki butun mamlakat iqtisodiy barqarorligi uchun ham hal qiluvchi ahamiyatga ega.

1. Asosiy xulosalar

Energetika va iqtisodiy barqarorlikka o'xshash tarzda, axborot xavfsizligi ham strategik resursdir. Agar iqtisodiy axborotlar xavfsizligi ta'minlanmasa, bu moliyaviy yo'qotishlarga, investitsiya muhitining yomonlashishiga va davlat darajasida iqtisodiy barqarorlikning izdan chiqishiga olib kelishi mumkin.

Tahdidlar ko'p qirrali. Tashqi tahdidlar — kiberhujumlar, xakerlik, zararli dasturlar; ichki tahdidlar — xodimlar tomonidan axborotlarni oshkor qilish, noto'g'ri foydalanish; tizimli muammolar — huquqiy tartibotlarning zaifligi va texnologik infratuzilmaning yetarli emasligi.

Himoya usullari samarali bo'lsa-da, kompleks yondashuv zarur. Kriptografiya, autentifikatsiya, tarmoq xavfsizligi, huquqiy mexanizmlar va xalqaro standartlar birgalikda qo'llanilgandagina iqtisodiy axborotlar xavfsizligi ta'minlanadi.

Xalqaro tajriba muhim. AQShda SOX va GLBA qonunlari, Yevropa Ittifoqida GDPR reglamenti, Yaponiya va Janubiy Koreyada kiberxavfsizlik strategiyalari iqtisodiy axborotlar xavfsizligini ta'minlashda samarali mexanizmlar sifatida ko'riladi.

O'zbekiston sharoitida muammolar mavjud. Kiberxavfsizlik bo'yicha xodimlar yetishmasligi, huquqiy tartibotlarning zaifligi, aholining kiberxavfsizlik bo'yicha xabardorlik darajasi pastligi va ma'lumotlarni saqlash infratuzilmasining yetarli emasligi asosiy muammolar sifatida qayd etildi.

2. Takliflar

Huquqiy mexanizmlarni kuchaytirish. O'zbekistonda iqtisodiy axborotlar xavfsizligini ta'minlash uchun maxsus qonunlar qabul qilinishi zarur. Masalan, moliyaviy hisobotlarning aniqligi va xavfsizligini ta'minlashga qaratilgan qonunlar, bank va moliyaviy institutlar tomonidan mijozlarning shaxsiy va moliyaviy ma'lumotlarini himoya qilishni majburiy qiluvchi normativ hujjatlar ishlab chiqilishi kerak.

Texnologik infratuzilmani rivojlantirish. Kriptografiya, autentifikatsiya, tarmoq xavfsizligi va xalqaro standartlar asosida zamonaviy texnologiyalar joriy etilishi zarur. ISO/IEC 27001 standarti asosida axborot xavfsizligini boshqarish tizimi yaratish va qo'llash muhimdir.

Kadrlar tayyorlash. Kiberxavfsizlik bo'yicha malakali mutaxassislar tayyorlash, universitetlarda maxsus yo'nalishlar ochish va xalqaro tajribani o'rganish zarur. Bu kadrlar iqtisodiy axborotlar xavfsizligini ta'minlashda muhim rol o'ynaydi.

Aholi xabardorligini oshirish. Kiberxavfsizlik bo'yicha keng qamrovli tushuntirish va xabardorlik kampaniyalari olib borish, aholining kiberxavfsizlik bo'yicha bilim va ko'nikmalarini oshirish zarur.

Davlat-xususiy sektor hamkorligini kengaytirish. Iqtisodiy axborotlar xavfsizligini ta'minlashda davlat va xususiy sektor hamkorligi muhimdir. Banklar, moliyaviy institutlar, korporatsiyalar va davlat organlari birgalikda ishlashi zarur.

Xalqaro hamkorlikni kuchaytirish. Iqtisodiy axborotlar xavfsizligini ta'minlashda xalqaro tajribani o'rganish, xalqaro standartlarga rioya qilish va xalqaro hamkorlikni kengaytirish zarur.

3. Yakuniy xulosa

Umuman olganda, iqtisodiy axborotlar xavfsizligi O‘zbekistonda iqtisodiy barqarorlikni ta’minlash, investitsiya muhitini yaxshilash va moliyaviy tizimni mustahkamlash uchun muhimdir. Shu sababli iqtisodiy axborotlar xavfsizligini ta’minlash uchun kompleks yondashuv zarur: huquqiy mexanizmlar, texnologik infratuzilma, kadrlar tayyorlash, aholining xabardorligini oshirish, davlat-xususiy sektor hamkorligi va xalqaro hamkorlik.

FOYDALANILGAN ADABIYOTLAR

1. ISO/IEC 27001: Information Security Management Systems — Requirements. International Organization for Standardization, 2022.
2. Sarbanes-Oxley Act (SOX). United States Congress, 2002.
3. Gramm-Leach-Bliley Act (GLBA). United States Congress, 1999.
4. General Data Protection Regulation (GDPR). European Union, 2018.
5. OECD. Digital Security Risk Management for Economic and Social Prosperity. OECD Publishing, 2021.
6. IMF. Cybersecurity and Financial Stability: Risks and Policy Responses. International Monetary Fund, 2023.
7. World Bank. Securing Digital Transformation in Emerging Economies. World Bank Report, 2022.
8. Ministry for Digital Development of Uzbekistan. National Cybersecurity Strategy, 2023.
9. Kaspersky Lab. Global Cybersecurity Report, 2024.
10. Symantec. Internet Security Threat Report, 2023.