

**KIBERXAVFSIZLIKNING IQTISODIY AHAMIYATI VA KORXONALAR UCHUN
XAVF TURLARI****Salomov Muhammadali Xusniyor o'g'li****Namangan davlat universiteti****Iqtisodiyot fakulteti 1-kurs talabasi****Email: Salomovmuhammadali0@gmail.com****Tel: +998992522973****Ubaydullayeva Diloromxon Maxmudjon qizi****Namangan davlat universiteti****Raqamli ta'lim texnologiyalar kafedrasi o'qituvchisi****E-mail: ubaydullayevadilorom378@gmail.com****Tel: +998940677715****<https://doi.org/10.5281/zenodo.17840273>**

Annotatsiya: Ushbu maqolada kiberxavfsizlikning zamonaviy iqtisodiyotdagi roli, korxonalarga kiberxavflarning ta'siri va ularni kamaytirish usullari ilmiy asosda tahlil qilinadi. Kiberxavfsizlikning iqtisodiy ahamiyati, moliyaviy zararlarni kamaytirish, ish jarayonlarining uzluksizligini ta'minlash va raqamli aktivlarni himoya qilish jihatlari ko'rib chiqiladi. Shuningdek, korxonalarda uchraydigan asosiy xavf turlari va ularni oldini olish strategiyalari bilan tanishtiriladi.

Kalit so'zlar: Kiberxavfsizlik, iqtisodiy zarar, korxona, axborot xavfsizligi, kiberxavf turlari, raqamli aktivlar, xavfni boshqarish

Kirish: Raqamli transformatsiya davrida korxonalar va moliyaviy institutlar o'z faoliyatini internet va raqamli tizimlarga ko'chirgan sari kiberxavfsizlik masalasi muhim ahamiyat kasb etadi [1]. Kiberhujumlar nafaqat moliyaviy zarar, balki obro' va mijozlar ishonchining yo'qolishiga olib keladi. Shu sababli, korxonalar iqtisodiy barqarorlikni ta'minlash uchun kiberxavfsizlikni strategik element sifatida qabul qilishi zarur [2].

KIBERXAVFSIZLIKNING IQTISODIY AHAMIYATI**Kiberxavfsizlik va moliyaviy barqarorlik**

Kiberxavfsizlik tizimlari korxonalarni moliyaviy zarar, tizim ishdan chiqishi va ma'lumot yo'qolishidan himoya qiladi. Tadqiqotlar shuni ko'rsatadiki, kiberxavfsizlik choralari ko'rgan korxonalar yiliga o'rtacha 30–40% kamroq moliyaviy zarar ko'radi [3].

Ish jarayonlarining uzluksizligi

Kiberhujumlar korxona faoliyatining to'xtashiga olib keladi, bu esa ishlab chiqarish, xizmat ko'rsatish va savdo jarayonlariga to'g'ridan-to'g'ri salbiy ta'sir ko'rsatadi. Shu bois, xavfsizlik tizimlari ish jarayonlarini uzluksiz ta'minlash va xarajatlarni kamaytirishda muhim rol o'ynaydi [4].

Raqamli aktivlarni himoya qilish

Korxonalar uchun raqamli aktivlar — bu mijozlar ma'lumotlari, moliyaviy hisob kitoblar, mahsulot va loyiha fayllari. Ularni yo'qotish yoki buzilish iqtisodiy yo'qotishlarga olib keladi [5].

KORXONALAR UCHUN KIBERXAVFLAR VA ULARNING TURLARI

Asosiy kiberxavf turlari

Xavf turi	Ta'rif	Iqtisodiy ta'siri
Phishing	Foydalanuvchini aldash orqali shaxsiy ma'lumotlarni olish	Moliyaviy yo'qotish, shaxsiy ma'lumotlar tarqalishi
Malware (virus, trojan)	Kompyuter tizimiga zarar yetkazadigan dastur	Ish jarayonining to'xtashi, ma'lumot yo'qolishi
Ransomware	Fayllarni shifrlash va pul talab qilish	Moliyaviy zarar, ishlab chiqarishning to'xtashi
DDoS hujumlari	Tarmoqni ishdan chiqarish	Veb-sayt va xizmatlar uzilishi, mijozlarning yo'qolishi
Ichki xodimlar xatolari	Ma'lumotni noto'g'ri ishlatish yoki yo'qotish	Moliyaviy yo'qotish, obro'ga zarar
Ma'lumotlar o'g'irligi	Raqamli aktivlarni o'g'irlash	Moliyaviy va strategik zara

Kiberxavflarni kamaytirish strategiyalari

- Xodimlarni kiberxavfsizlik bo'yicha o'qitish;
- Antivirus va firewall tizimlarini yangilash;
- Ma'lumotlarni muntazam zaxiralash;
- Kiritilgan tizimlarga kirishni nazorat qilish;
- Kiberhujumlar bo'yicha tezkor javob jamoasini yaratish [6].

KIBERXAVFSIZLIKNING IQTISODIY SAMARADORLIGI

1. Moliyaviy zararlarni kamaytiradi.
2. Ish jarayonini uzluksiz ta'minlaydi.
3. Raqamli aktivlarni himoya qiladi.
4. Korxona obro'si va mijozlar ishonchini saqlaydi.
5. Strategik qarorlar qabul qilish uchun ma'lumotlarni xavfsiz saqlaydi [3]/[5].

Xulosa: Kiberxavfsizlikning iqtisodiy ahamiyati korxonalarda strategik qarorlar qabul qilish, moliyaviy barqarorlikni ta'minlash va raqamli aktivlarni himoya qilish bilan bevosita bog'liq. Tadqiqotlar shuni ko'rsatadiki, kiberxavfsizlik choralari yetarli darajada joriy etmagan korxonalar yillik daromadining sezilarli qismini kiberhujumlar, ma'lumot yo'qotish, ish jarayonining uzilishi va mijozlarning ishonchining pasayishi orqali yo'qotadi. Shuningdek, kiberxavfsizlik tizimlarini rivojlantirish va zamonaviy standartlarga moslash korxonaga bir necha jihatdan iqtisodiy foyda keltiradi:

1. **Moliyaviy zararlarni kamaytirish** – antivirus, firewall, ERI tizimi va ma'lumotlarni zaxiralash kabi choralar yordamida kiberhujumlar natijasida yuzaga keladigan moliyaviy yo'qotishlar kamayadi.

2. Ish jarayonining uzluksizligini ta'minlash – kiberhujumlar va tizim xatoliklari tufayli ishlab chiqarish yoki xizmat ko'rsatish jarayonlarining to'xtashini oldini oladi, shu bilan daromad va mijozlar ishonchi saqlanadi.

3. Raqamli aktivlarni himoya qilish – korxonaning strategik va moliyaviy ma'lumotlari, patentlar, mijozlar bazasi va mahsulot ma'lumotlari xavfsiz saqlanadi, bu esa uzoq muddatli iqtisodiy barqarorlikni kafolatlaydi.

4. Korxona obro'si va raqobatbardoshligini oshirish – mijozlar va hamkorlar ma'lumotlarining xavfsizligi ta'minlangan korxonaga ko'proq ishonadi, bu esa bozor pozitsiyasini mustahkamlaydi.

5. Xavflarni boshqarish tizimini takomillashtirish – kiberxavfsizlik strategiyasi orqali korxona risklarni oldindan aniqlab, tezkor choralar ko'rish imkoniyatiga ega bo'ladi.

Umuman olganda, kiberxavfsizlik – bu nafaqat texnologik masala, balki korxonaning iqtisodiy barqarorligini, samaradorligini va uzoq muddatli rivojlanishini ta'minlovchi muhim strategik vosita hisoblanadi. Bugungi kunda raqamli transformatsiya jarayonida kiberxavfsizlikni e'tibordan chetda qoldirmaslik, investitsiya qilish va xodimlar savodxonligini oshirish korxonaning kelajakdagi muvaffaqiyati va iqtisodiy samaradorligini kafolatlaydi.

Adabiyotlar, References, Литературы:

1. He, W., & Yan, G. (2021). Economic Impact of Cybersecurity in Enterprises. Journal of Information Security.
2. O'zbekiston Respublikasi Raqamli Texnologiyalar Vazirligi Statistik Ma'lumotlari, 2023.
3. Smith, J. (2020). Cybersecurity and Economic Stability. International Journal of IT & Business.
4. ENISA. (2022). Threat Landscape Report.
5. Kaspersky Lab Reports (2021). Global Corporate Cyber Threats.
6. Ponemon Institute. (2020). Cost of Cybercrime Study.