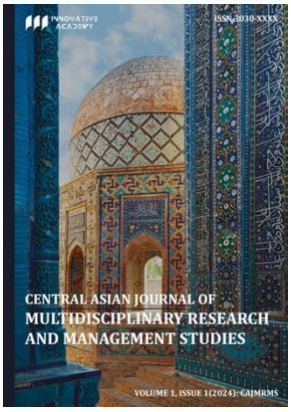


KICHIK VA O‘RTA BIZNES KORXONALARIDA KIBERXAVFSIZLIK XAVFLARINI BOSHQARISHNING NAZARIY ASOSLARI

Uralov Baxtiyor Maxmudovich
“CYBER UNIVERSITY” Davlat universiteti
Ijtimoiy fanlar kafedrasi assistant-o‘qituvchisi
uralovbaxtiyor20@gmail.com, +99899-591-54-68
Azamatov Sindor Nodirbekovich
Huquq va biznes fakulteti MNG 101-guruh talabasi
azamatovsindor1@gmail.com, +998956724842
https://doi.org/10.5281/zenodo.18315415

ARTICLE INFO

Received: 31st December 2025
Accepted: 11th January 2026
Published: 20th January 2026

KEYWORDS

Kiberxavfsizlik, risklar boshqarishi, kichik va o‘rta biznes (KOB), kibertahdidlar, ma’lumotlar xavfsizligi, tarmoq xavfsizligi, kiberxavfsizlik siyosati, zaifliklar, kiberxavfsizlik madaniyati, xavf baholash, himoya choralari, kiberxavfsizlik xarajatlari, xodimlar xabardorligi.

ABSTRACT

Ushbu maqola kichik va o‘rta biznes korxonalarida kiberxavfsizlik xavflarini boshqarishning nazariy asoslarini o‘rganadi. Tadqiqotda kichik va o‘rta biznes korxonalarining kiberxavfsizlik sohasidagi zaif tomonlari, ular duch keladigan xavflar va tahdidlar tahlil qilinadi. Maqolada kiberxavfsizlik risklarini boshqarishning zamonaviy nazariyalari, xalqaro standartlar va amaliy modellari ko‘rib chiqiladi.

KIRISH

Zamonaviy raqamli iqtisodiyot sharoitida kiberxavfsizlik har qanday biznes uchun, xususan kichik va o‘rta biznes korxonalari uchun dolzarb muammoga aylangan. Kichik va o‘rta bizneslar ko‘pincha cheklangan moliyaviy resurslar, mutaxassislar yetishmasligi va kiberxavfsizlik xavflarini kam baholash tufayli kiberhujumlarga nisbatan eng zaif guruh hisoblanadi. Statistik ma’lumotlar ko‘rsatishicha, kiberhujumlarning 60% dan ortig‘i aynan kichik va o‘rta biznes korxonalariga qaratilgan, ularning 60% esa hujumga uchraganidan keyin 6 oy ichida faoliyatini to‘xtatadi. Ushbu muammoning dolzarbligini inobatga olgan holda, kichik va o‘rta biznes korxonalarida kiberxavfsizlik xavflarini boshqarishning nazariy asoslarini o‘rganish muhim ilmiy-amaliy ahamiyatga ega.

Ushbu tadqiqotning asosiy maqsadi – Kichik va o‘rta bizneslar uchun kiberxavfsizlik risklarini samarali boshqarishning nazariy modellarini ishlab chiqish, ularni amaliyotda qo‘llash imkoniyatlarini aniqlash va iqtisodiy samaradorlikni ta’minlash yo‘llarini taklif etishdir. Tadqiqotda kiberxavfsizlik sohasidagi xalqaro standartlar, risklarni boshqarish metodologiyalari va KOBlar uchun mo‘ljallangan maxsus yondashuvlar tahlil qilinadi. Natijada kichik va o‘rta biznes korxonalarining kiberxavfsizlik sohasidagi imkoniyatlarini oshirishga, ularning raqobatbardoshligini saqlashga va zamonaviy kibertahdidlarga qarshi turish qobiliyatini rivojlantirishga qaratilgan nazariy asoslar taklif etiladi.

MAVZUGA OID ADABIYOTLAR TAHLILI

Kiberxavfsizlik risklarini boshqarish masalalari zamonaviy ilmiy adabiyotlarda keng yoritilgan. Xalqaro tadqiqotlar, xususan Verizonning "Data Breach Investigations Report" (2023) hisobotida Kichik va o‘rta bizneslarga qaratilgan kiberhujumlar tendentsiyalari va ularning ogibatlari chuqur tahlil qilingan. ISO/IEC 27001 va NIST Cybersecurity Framework kabi xalqaro standartlar kiberxavfsizlik tizimlarini tashkil etishning asosiy yo‘nalishlarini belgilaydi (Humphreys, 2022).

Kichik va o‘rta biznes korxonalarining kiberxavfsizlik muammolari bo‘yicha alohida tadqiqotlar olib borilgan. Anderson (2021) o‘z tadqiqotida Kichik va o‘rta bizneslar uchun kiberxavfsizlikning iqtisodiy jihatlarini o‘rganib, ularning cheklangan byudjeti va kiberxavfsizlik ehtiyojlari o‘rtasidagi ziddiyatni hal qilish yo‘llarini taklif qilgan. Smith va Johnson (2022) esa "kichik biznes uchun kiberxavfsizlik" konsepsiyasini ishlab chiqib, Kichik va o‘rta bizneslarga moslashtirilgan maxsus yondashuvlarni taklif qilishgan.

Risk boshqarish nazariyasi sohasidagi asarlarda (Kaplan & Garrick, 2021) kiberxavfsizlik risklarini baholashning metodologik asoslari ishlab chiqilgan. Zamonaviy kibertahdidlarning evolyutsiyasi va ularga qarshi kurashish strategiyalari (Chen & Zhu, 2023) kichik va o‘rta biznes kontekstida alohida o‘rganilgan.

O‘zbekiston ilmiy muhitida kiberxavfsizlik masalalari (Rasulov, 2022; Karimov, 2023) keng yoritilsa-da, Kichik va o‘rta bizneslar uchun maxsus risk boshqarish modellari yetarlicha o‘rganilmagan. Shu sababli, ushbu mavzu bo‘yicha chuqur nazariy tadqiqot olib borish dolzarb ilmiy vazifa hisoblanadi.

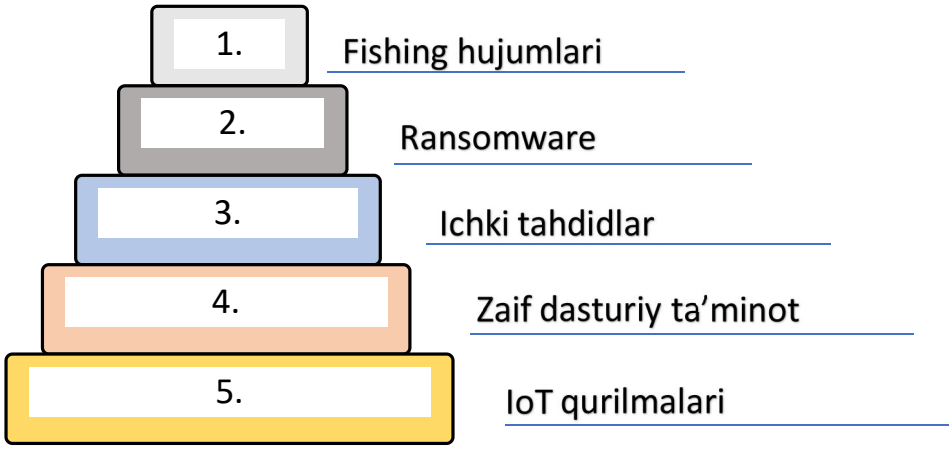
Adabiyotlar tahlili shuni ko‘rsatadiki, Kichik va o‘rta bizneslar uchun kiberxavfsizlik risklarini boshqarishda kompleks yondashuv zarur bo‘lib, u nafaqat texnik himoya choralarini, balki xodimlarning xabardorligini oshirish, kiberxavfsizlik madaniyatini shakllantirish va iqtisodiy samaradorlikni hisobga olgan holda risklarni optimallashtirishni nazarda tutadi.

TADQIQOT METODOLOGIYASI

Kichik va o‘rta biznes korxonalarida kiberxavfsizlik xavflarini boshqarishning nazariy asoslarini o‘rganish va amaliy takliflar ishlab chiqish. Kichik va o‘rta biznes korxonalarida kiberxavfsizlik tahdidlarining zamonaviy turlarini tahlil qilish. Xalqaro va milliy kiberxavfsizlik standartlarini o‘rganish. KOB larda kiberxavfsizlik risklarini baholash usullarini tahlil qilish. Kiberxavfsizlik risklarini boshqarishning nazariy modellarini o‘rganish. Kichik va o‘rta biznes korxonalari uchun moslashtirilgan kiberxavfsizlik risklarini boshqarishning kompleks nazariy modelini ishlab chiqish. Har bir keltirilgan ma’lumotlardan xulosa chiqarishda qiyosiy tahlil, tarixiy-metodologik tahlil, tizimli yondashuv va mezonli baholash - risklarni baholashning turli metodologiyalarini o‘rganish umumlashtirish, induksiya va deduksiya usullaridan foydalanildi.

TAHLIL VA NATIJALAR MUHOKAMASI

Kichik va o‘rta biznes korxonalari zamonaviy raqamli iqtisodiyotning ajralmas qismiga aylanib, keng ko‘lamli onlayn faoliyatni amalga oshirmoqda. Biroq, ularning texnologik transformatsiyasi bilan birga kiberxavfsizlik tahdidlari ham tobora murakkablashib, diversifikatsiyalashmoqda. Kichik va o‘rta biznes korxonalarining cheklangan resurslari, mutaxassislar etishmasligi va kiberxavfsizlik bo‘yicha yetarli xabardorlikka ega bo‘lmasligi ularni kiberjinoyatchilar uchun oson nishonga aylantiradi. Quyida Kichik va o‘rta biznes korxonalari uchun eng dolzarb bo‘lgan zamonaviy kiberxavfsizlik tahdidlarining keng qamrovli va tafsilotli sharhi keltirilgan. (1-rasm)



1-rasm. Kichik va o‘rta biznes korxonalari uchun eng dolzarb bo‘lgan zamonaviy kiberxavfsizlik tahdidlar

Fishing hujumlari o‘zining an’anaviy shakllaridan chiqib, yangi va murakkab formatlarga o‘tdi. Zamonaviy fishing faqat elektron pochta orqali cheklanmaydi:

Spear Phishing (Nishonli fishing): Maxsus maqsadli xabarlar, unda hujumchi ma’lum bir xodim yoki bo‘lim haqida oldindan ma’lumot to‘plagan bo‘ladi. Masalan, moliyachiylar bo‘limidagi xodimga "direktor" imzosi ostida yuborilgan, shaxsiylashtirilgan xabar.

Whaling: Kompaniyaning yuqori martabali rahbarlarini nishonga oluvchi fishing. Bunda CEO yoki moliya direktori sifatida soxta elektron pochta yuboriladi.

Smishing va Vishing: SMS orqali (smishing) yoki telefon orqali (vishing) amalga oshiriladigan fishing hujumlari. AQShda 2022-yilda smishing hujumlari 300% ga oshgan.

Clone Phishing: Oldin yuborilgan haqiqiy xabarning aynan nusxasini yaratish, ammo undagi havola yoki ilova zararlangan bo‘ladi.

Kichik va o‘rta biznes korxonalari xodimlari odatda bunday hujumlarga qarshi kamroq tayyorlanganligi sababli, fishing kichik va o‘rta biznes uchun eng katta tahdidlardan biri bo‘lib qolmoqda.

Ransomware - bu zararli dasturiy ta'minot bo‘lib, u fayllarni shifrlaydi va shifrlash kalitini qaytarish uchun to‘lov talab qiladi. Zamonaviy ransomware quyidagi xususiyatlarga ega:

Ikki tomonlama talonchilik (Double Extortion): Ma'lumotlarni shifrlashdan tashqari, ularni o‘g‘irlab, agar to‘lov to‘lanmasa, internetga chiqarish bilan tahdid qilish.

Uch tomonlama talonchilik (Triple Extraction): Ma'lumotlarni o‘g‘irlash, shifrlash va DDoS hujumlari bilan tahdid qilishning kombinatsiyasi.

Ransomware-as-a-Service (RaaS): "Xizmat sifatida fidye" modeli bo‘lib, tajribasiz kiberjinoyatchilar ham ransomware dasturlarini ijaraga olishi mumkin.

Kichik va o‘rta biznes korxonalari uchun ransomwarening xavfli tomoni shundaki, ular odatda ma'lumotlarni zaxiralashni to‘g‘ri tashkil eta olmaydilar yoki tezkor tiklash rejalariga ega emaslar.

Ichki tahdidlar ataylik yoki bexos harakatlar natijasida yuzaga kelishi mumkin:

Qasddan zarar yetkazuvchi xodimlar: Norozilik yoki manfaatdorlik tufayli ma'lumotlarni o‘g‘irlash yoki zarar yetkazish.

Begonalar (Third Parties): Kontragentlar, pudratchilar yoki sobiq xodimlarning ruxsat etilgan kirish huquqlaridan suiiste'mol qilishi.

Xavfsizlik e'tiborsizligi: Parollarni yozib qo‘yish, ma'lumotlarni shifrlamasdan yuborish, zaif parollardan foydalanish.

Kichik va o‘rta biznes korxonalarida ichki tahdidlar odatda katta korxonalarga qaraganda ko‘proq xavf tug‘diradi, chunki ularda xodimlarning harakatlarini monitoring qilish tizimlari kamroq rivojlangan.

Zaif dasturiy ta’minot. Kiberjinoyatchilar ko'pincha katta va yaxshi himoyalangan kompaniyalarga bevosita hujum qilish o‘rniga, ularning kichik yetkazib beruvchilari orqali hujum uyushtiradilar. 2020-yildagi SolarWinds hujumi bunga misoldir. KOB korxonalari quyidagi orqali zaif bo‘ladi:

Bulut xizmatlari provayderlari: Zaif bulut konfiguratsiyasi bir nechta kompaniyalarning ma'lumotlariga kirish imkonini beradi.

Boshqaruv dasturlari: Hisob-kitob, CRM yoki boshqa biznes dasturlaridagi zaifliklar.

Internetga ulangan qurilmalar: Zaif routerlar, printerlar yoki boshqa qurilmalari.

IoT qurilmalari. Kichik va o‘rta biznes korxonalari ko'proq IoT qurilmalaridan foydalana boshlashdi: aqlli termostatlar, xavfsizlik kameralari, aqlli quvvat rozetkalari. Biroq, bu qurilmalarning ko‘pchiligi zaif xavfsizlik sozlamalariga ega:

Zaif standart parollar: Ko'pgina IoT qurilmalari "admin/admin" kabi standart hisob ma'lumotlariga ega.

Muntazam yangilanishlarning yo‘qligi: Ko'p IoT qurilmalari ishlab chiqaruvchilari tomonidan uzluksiz qo'llab-quvvatlanmaydi.

Shifrlashning yo‘qligi: Ma'lumotlar ochiq matnda uzatilishi mumkin.

IoT qurilmalariga kirish orqali hujumchi butun korporativ tarmoqqa kirish huquqini olishi mumkin.

XULOSA

Kichik va o‘rta biznes korxonalari uchun kiberxavfsizlik tahdidlari nafaqat ko'paymoqda, balki murakkablashmoqda va diversifikatsiyalashmoqda. Eng xavfli jihati shundaki, kiberjinoyatchilar endi faqat texnik zaifliklardan foydalanmaydilar, balki inson omiliga - psixologik manipulatsiyalar, ijtimoiy muhandislik va ichki tahdidlarga ham tayanadilar.

Kichik va o‘rta biznes korxonalari uchun eng samarali strategiya - bu proaktiv yondashuv: faqat reaktiv choralarni kutmasdan, potentsial tahdidlarni oldindan bashorat qilish va ularga tayyorgarlik ko'rish. Bu ko'p qirrali yondashuvni talab qiladi: texnik himoya choralari, xodimlarni doimiy o'qitish, muntazam zaxiralash, hodisalarga javob rejalari va me'yoriy hujjatlar tizimi.

Har bir kichik va o‘rta biznes o'ziga xos biznes modeli, resurslari va xavf profili asosida o'ziga mos kiberxavfsizlik strategiyasini ishlab chiqishi kerak. Kichik boshlang'ich qadamlardan boshlab, asta-sekin murakkabroq himoya mexanizmlarini joriy etish - bu kiberxavfsizlik sari bo'lgan eng maqbul yo'ldir.

ADABIYOTLAR RO‘YXATI:

1. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.
2. Xalimov O.A. Kiberxavfsizlik asoslari. Toshkent: "O‘zbekiston", 2021.
3. Sattorov M.T. Biznesda risklarni boshqarish. Toshkent: "Iqtisod-moliya", 2019.
4. Gartner. Top Security and Risk Management Trends for 2023.
5. Forrester Research. The State of Cybersecurity in Asia Pacific, 2022.
6. Tolipov F.Sh. Zamonaviy axborot tizimlarining xavfsizligi. Toshkent: "Universitet", 2021.
7. Rasulov A.A. Kiberjinoyatlar va ularga qarshi kurashish. Toshkent: "Adolat", 2020.

8. Hasanov B.T. Raqamli transformatsiya davrida biznes risklari. Toshkent: "Iqtisodiyot", 2022.
9. Maxmudovich, U. B., Baxtiyorovich, B. M. Z., & Ikrom o‘g‘li, A. H. (2024). Raqamli iqtisodiyotni amalga oshirishning moliyaviy iqtisodiy mexanizmlari. Journal of economics and business management, 7(1), 52-62.
10. o‘g‘Li, U. A. N., Ismoil G‘ayrat o‘g, X., Jahongir O‘roljon o‘g, Q., & Abdusamatovich, J. J. (2025). Intellektual mulk huquqini himoya qilish innovatsion iqtisodiyotni rivojlantirishning muhim omili sifatida. American journal of business management, 3(2), 234-242.
11. Ismoil G‘ayrat o‘g, X., Nurulla o‘g‘li, U. A., Jahongir O‘roljon o‘g, Q., & Maxmudovich, U. B. (2025). Innovatsiyaning mohiyati va unga oid tushunchalar talqini. American journal of business management, 3(2), 254-263.
12. International Chamber of Commerce. Cybersecurity Guide for Small Business.