INNOVATIVE PUBLICATION

Journal of Effective Learning and Sustainable Innovation

Vol.4 №11 (2026). NOVEMBER

innovativepublication.uz

ENHANCING BUSINESS COMPETITIVENESS THROUGH CYBERSECURITY STRATEGIES

Bahodirov Jahongirmirzo Baxriddin o‘g‘li

Fourth-Year Student, Millat Umidi University

Phone: +998 (93) 127-40-34
E-mail: jahongirmirzobahodirov227@gmail.com

Scientific Supervisor: Dinara Ishmanova

KIBERXAVFSIZLIK STRATEGIYALARI ORQALI KORXONALARNING RAQOBATBARDOSHLIGINI OSHIRISH.

Ilmiy rahbar: **Ishmanova Dinara**
Millat Umidi universitetining 4-kurs talabasi
Bahodirov Jahongirmirzo Baxriddin o’g’li
+998(93)127-40-34, jahongirmirzobahodirov227@gmail.com

Annotatsiya: Ushbu maqolada zamonaviy korxonalar faoliyatida kiberxavfsizlikning ahamiyati va uning raqobatbardoshlikni oshirishdagi o‘rni yoritilgan. Shuningdek, korxonalarda axborotlarni himoya qilish, kiberhujumlarning oldini olish, xodimlarning kiberxavfsizlik bo‘yicha bilimlarini oshirish va zamonaviy himoya texnologiyalaridan foydalanish masalalari tahlil qilingan. Mavjud muammolarni bartaraf etish bo‘yicha takliflar ishlab chiqilgan hamda kiberxavfsizlik strategiyalarini samarali qo‘llash orqali korxonalarning bozordagi mavqeini mustahkamlash imkoniyatlari ko‘rib chiqilgan.

Kalit so‘zlar: kiberxavfsizlik, korxona, raqobatbardoshlik, axborot xavfsizligi, kiberhujumlar, raqamli iqtisodiyot, ma’lumotlarni himoya qilish, zamonaviy texnologiyalar, biznes strategiyasi, axborot tizimlari.

Аннотация: В статье подчеркивается значимость кибербезопасности в деятельности современных предприятий и ее роль в повышении конкурентоспособности. Также анализируются вопросы, связанные с защитой информации, предотвращением кибератак, повышением уровня знаний сотрудников в области кибербезопасности и использованием современных технологий защиты. Предлагаются меры по решению существующих проблем, а

также рассматриваются возможности укрепления рыночных позиций предприятия за счет эффективной реализации стратегий кибербезопасности.

Ключевые слова: кибербезопасность, предприятие, конкурентоспособность, информационная безопасность, кибератаки, цифровая экономика, защита данных, современные технологии, бизнес-стратегия, информационные системы.

Annotation: This article highlights the importance of cyber security in the operation of modern enterprises and its role in increasing competitiveness. In addition, issues of information protection, prevention of cyber attacks, improvement of employees' knowledge of cyber security and use of modern protection technologies were analyzed. Proposals for solving existing problems were developed, and the possibilities of strengthening the position of enterprises in the market through the effective use of cyber security strategies were considered.

Keywords: cybersecurity, enterprise, competitiveness, information security, cyberattacks, digital economy, data protection, modern technologies, business strategy, information systems.

Kirish: Bugungi kunda raqamli texnologiyalar tez sur’atlar bilan rivojlanib, korxonalar faoliyatiga keng kirib bormoqda. Hozirgi vaqtda ko‘plab korxonalar o‘z ish jarayonlarini boshqarish, mijozlar bilan aloqa o‘rnatish, to‘lovlarni amalga oshirish va ma’lumotlarni saqlashda internet hamda turli axborot tizimlaridan foydalanmoqda. Bu esa korxonalar faoliyatini tezlashtirish va samaradorlikni oshirishga yordam bermoqda. Shu bilan birga, raqamli texnologiyalardan foydalanish jarayonida kiberhujumlar, ma’lumotlarning o‘g‘irlanishi va axborot tizimlariga noqonuniy kirish kabi xavflar ham ortib bormoqda. Ayniqsa, korxonalar uchun mijozlarning shaxsiy ma’lumotlari, moliyaviy hujjatlar va tijorat sirlarini himoya qilish muhim ahamiyatga ega. Chunki bunday ma’lumotlarning yo‘qolishi yoki begona shaxslar qo‘liga tushishi korxonaga katta moliyaviy zarar yetkazishi, uning obro‘siga salbiy ta’sir qilishi mumkin. Natijada mijozlar ishonchi pasayib, korxonaning bozordagi raqobatbardoshligi zaiflashadi. Shu sababli korxonalarda kiberxavfsizlik strategiyalarini ishlab chiqish va ularni amaliyotga joriy etish bugungi kunning dolzarb masalalaridan biri hisoblanadi. Bunda zamonaviy himoya dasturlaridan foydalanish, xodimlarning axborot xavfsizligi bo‘yicha bilimlarini oshirish va ma’lumotlarni muntazam nazorat qilish muhim o‘rin tutadi. Mazkur mavzuning dolzarbligi shundaki, kiberxavfsizlikni to‘g‘ri tashkil etish korxonalarga nafaqat turli xavflardan himoyalanish, balki mijozlar ishonchini oshirish, faoliyat barqarorligini ta’minlash va bozorda boshqa korxonalardan ustunlikka erishish imkonini beradi. Shu jihatdan kiberxavfsizlik strategiyalarini korxonalarning umumiy

rivojlanish rejasi bilan bog‘liq holda o‘rganish muhim hisoblanadi.

Adabiyotlarning tahlili: Kiberxavfsizlik va uning korxonalar faoliyatiga ta’siri bugungi kunda ko‘plab xorijiy va mahalliy mutaxassislar tomonidan o‘rganilayotgan dolzarb mavzulardan biri hisoblanadi. Raqamli texnologiyalar rivojlanishi bilan korxonalarda axborotlarni himoya qilish, ma’lumotlar xavfsizligini ta’minlash va kiberhujumlarning oldini olish masalalariga bo‘lgan e’tibor ortib bormoqda. Jahon iqtisodiy forumining 2025-yildagi *Global Cybersecurity Outlook* hisobotida kiberxavfsizlikning iqtisodiy barqarorlik va korxonalar faoliyatidagi ahamiyati yoritilgan. Unda kichik tashkilotlarning 35 foizi o‘z kiberxavfsizlik imkoniyatlarini yetarli deb hisoblamasligi ta’kidlangan. Bu esa korxonalarda axborot xavfsizligini kuchaytirish va zamonaviy himoya tizimlarini joriy etish zarurligini ko‘rsatadi. IBM kompaniyasining 2025-yilgi *Cost of a Data Breach Report* hisobotida ma’lumotlar buzilishi natijasida korxonalar ko‘radigan moliyaviy zararlar tahlil qilingan. Hisobotga ko‘ra, 2025-yilda ma’lumotlar buzilishining global o‘rtacha qiymati 4,44 million AQSH dollarini tashkil etgan. Bu ko‘rsatkich kiberxavfsizlikka e’tibor bermaslik korxonalar uchun katta iqtisodiy yo‘qotishlarga olib kelishi mumkinligini ko‘rsatadi. Shuningdek, ISO/IEC 27001 xalqaro standarti korxonalarda axborot xavfsizligini boshqarish tizimini tashkil etish bo‘yicha muhim talablarni belgilaydi. Ushbu standartda ma’lumotlarni himoya qilish, xavflarni baholash va axborot xavfsizligini doimiy nazorat qilish masalalariga alohida e’tibor qaratilgan. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonunida ham axborot tizimlari va resurslarini himoya qilish, kiberxavfsizlikni ta’minlash hamda mavjud tahdidlarning oldini olish bo‘yicha huquqiy asoslar belgilangan.

Tadqiqot metodologiyasi: Kiberxavfsizlik strategiyalarining korxonalar raqobatbardoshligini oshirishdagi o‘rni, qo‘llanish yo‘nalishlari va samaradorligi haqida ilmiy maqolalar, xalqaro hisobotlar hamda statistik ma’lumotlar o‘rganildi. Shu bilan birga, tahliliy usul, solishtirma tahlil, empirik va tizimli yondashuv metodlaridan foydalanildi.

Tahlil va natijalar: Bugungi kunda raqamli texnologiyalarning rivojlanishi korxonalar faoliyatida kiberxavfsizlikning ahamiyatini yanada oshirmoqda. Chunki korxonalar o‘z faoliyatida mijozlar ma’lumotlari, moliyaviy hujjatlar va boshqa muhim axborotlarni elektron tizimlarda saqlaydi. Ushbu ma’lumotlarning xavfsizligini ta’minlash korxonaning barqaror ishlashi va raqobatbardoshligini oshirishda muhim ahamiyatga ega. Tahlillar shuni ko‘rsatadiki, kiberhujumlar natijasida korxonalar moliyaviy zarar ko‘rishi, mijozlar ma’lumotlarini yo‘qotishi va bozordagi obro‘siga putur yetishi mumkin. IBM kompaniyasining 2025-yilgi hisobotiga ko‘ra, ma’lumotlar

buzilishining global o‘rtacha qiymati 4,44 million AQSH dollarini tashkil etgan. Bu esa korxonalar uchun kiberxavfsizlikka oldindan e’tibor qaratish qanchalik muhimligini ko‘rsatadi. Korxonalarda kiberxavfsizlikni ta’minlash orqali bir nechta ijobiy natijalarga erishish mumkin. Jumladan, mijozlarning shaxsiy ma’lumotlari himoyalanadi, moliyaviy yo‘qotishlar kamayadi, ish jarayonlarining uzluksizligi ta’minlanadi va mijozlar ishonchi ortadi. Bu omillar korxonaning bozordagi mavqeini mustahkamlashga yordam beradi. Shuningdek, zamonaviy himoya dasturlaridan foydalanish, xodimlarning bilimini oshirish va axborot tizimlarini muntazam tekshirib borish kiberxavflarni kamaytirishda muhim o‘rin tutadi. Ayniqsa, kichik va o‘rta korxonalar uchun bunday choralarni bosqichma-bosqich amalga oshirish foydali hisoblanadi. O‘rganishlar natijasida shuni ko‘rish mumkinki, kiberxavfsizlik strategiyalarini to‘g‘ri tashkil etgan korxonalar o‘z faoliyatidagi xavflarni kamaytirish bilan birga, mijozlar ishonchini qozonish va raqobatchilar orasida ustunlikka erishish imkoniyatiga ega bo‘ladi.

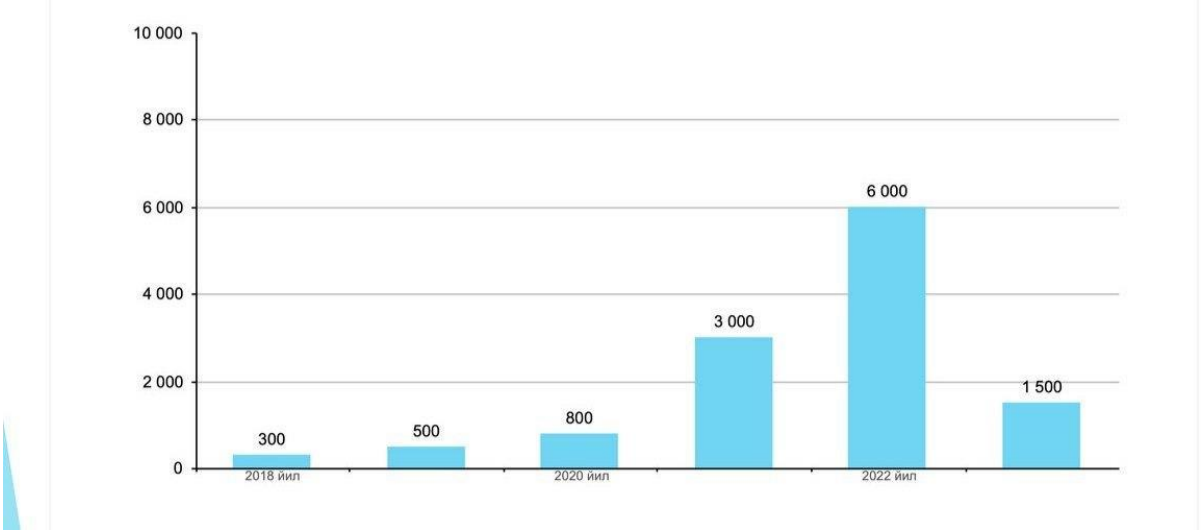
Kiberxavfsizlik strategiyalari orqali korxonalarning raqobatbardoshligini oshirish afzalliklari: Korxonalarda kiberxavfsizlik strategiyalarini joriy etish bir qator afzalliklarni yaratadi. Eng avvalo, korxonaning muhim ma’lumotlari va mijozlarning shaxsiy axborotlari himoyalanadi. Bu esa ma’lumotlarning yo‘qolishi yoki begona shaxslar qo‘liga tushishining oldini oladi. Yana bir muhim afzalligi — mijozlar ishonchining oshishidir. Chunki mijozlar o‘z ma’lumotlari xavfsiz saqlanadigan va to‘lov jarayonlari himoyalangan korxonalardan foydalanishni afzal ko‘radi. Natijada korxona yangi mijozlarni jalb qilish va mavjud mijozlarini saqlab qolish imkoniyatiga ega bo‘ladi. Shuningdek, kiberxavfsizlik moliyaviy yo‘qotishlarni kamaytirishga yordam beradi. Kiberhujumlar va axborot tizimidagi nosozliklarning oldini olish orqali korxona qo‘shimcha xarajatlarni kamaytirishi mumkin. Bundan tashqari, ish jarayonlarining uzluksizligi ta’minlanib, xodimlarning samarali ishlashi uchun sharoit yaratiladi. Kiberxavfsizlik strategiyalarining yana bir afzalligi korxonaning bozordagi obro‘sini mustahkamlashidir. Axborot xavfsizligiga jiddiy e’tibor beradigan korxonalar hamkorlar va investorlar oldida ishonchli tashkilot sifatida namoyon bo‘ladi. Bu esa yangi hamkorlik imkoniyatlarini yaratadi. Umuman olganda, kiberxavfsizlik strategiyalaridan samarali foydalanish korxonalarga xavflarni kamaytirish, mijozlar ishonchini oshirish, moliyaviy barqarorlikni saqlash va raqobatchilar orasida ustunlikka erishish imkonini beradi.

Kiberxavfsizlik strategiyalari orqali korxonalarning raqobatbardoshligini oshirish kamchiliklari: Korxonalarda kiberxavfsizlik strategiyalarini joriy etish ko‘plab afzalliklarga ega bo‘lsa-da, ayrim kamchilik va qiyinchiliklarni ham keltirib chiqaradi.

Birinchi navbatda, zamonaviy himoya dasturlari va texnologiyalarini sotib olish katta mablag‘ talab qiladi. Ayniqsa, kichik va o‘rta korxonalar uchun bunday xarajatlarni qoplash qiyin bo‘lishi mumkin. Yana bir kamchilik — malakali kiberxavfsizlik mutaxassislarining yetishmasligidir. Himoya tizimlarini to‘g‘ri boshqarish va nazorat qilish uchun maxsus bilim va tajriba talab etiladi. Bunday mutaxassislarni ishga olish esa korxona xarajatlarini oshiradi. Shuningdek, xavfsizlik tizimlarini doimiy yangilab borish va nazorat qilish qo‘shimcha vaqt hamda mehnat talab qiladi. Ayrim hollarda kuchli himoya cheklovlari xodimlarning ish jarayonini sekinlashtirishi va ayrim operatsiyalarni bajarishni murakkablashtirishi mumkin. Bundan tashqari, barcha xavfsizlik choralariga qaramay, kiberhujumlar xavfini butunlay yo‘qotib bo‘lmaydi. Yangi texnologiyalar bilan birga yangi kiberxavflar ham paydo bo‘lib boradi. Shu sababli korxonalar himoya tizimlarini muntazam takomillashtirib borishga majbur bo‘ladi. Umuman olganda, kiberxavfsizlik strategiyalarini joriy etish moliyaviy xarajatlar, mutaxassislar yetishmasligi va doimiy nazorat zarurati kabi qiyinchiliklarni yuzaga keltiradi. Shunga qaramay, bu kamchiliklar korxonaning uzoq muddatli xavfsizligi va rivojlanishi uchun muhim bo‘lgan himoya choralaridan voz kechishga sabab bo‘lmasligi kerak.



1- rasm. Tarixdagi eng katta axborot ma’lumotlarning buzilishlari 10 taligi kompaniyalar misolida.



2- Rasm. Toshkent shaxrida sodir etilgan kibrjinoyatlar.

Takliflar: Yuqoridagi maqola yozish uchun izlanishlarimdan kelib chiqib, bir nechta takliflarni taqdim eta olaman. Korxonalarda kiberxavfsizlikni kuchaytirish va raqobatbardoshlikni oshirish uchun, avvalo, axborot xavfsizligiga alohida e’tibor qaratish lozim. Buning uchun quyidagi takliflarni amalga oshirish maqsadga muvofiq: Birinchidan, har bir korxonada kiberxavfsizlik uchun alohida mablag‘ ajratish va zamonaviy himoya dasturlarini bosqichma-bosqich joriy etish kerak. Ikkinchidan, xodimlarning kiberxavfsizlik bo‘yicha bilimlarini oshirish maqsadida muntazam o‘quv mashg‘ulotlari tashkil etish lozim. Bu orqali fishing xabarlari, zararli havolalar va boshqa kiberxavflarning oldini olish mumkin. Uchinchidan, korxonalarda mijozlar va xodimlarning shaxsiy ma’lumotlarini himoya qilish uchun ikki bosqichli tasdiqlash tizimidan foydalanishni kengaytirish zarur. To‘rtinchidan, axborot tizimlarini muntazam tekshirib borish, dasturlarni o‘z vaqtida yangilash va muhim ma’lumotlarning zaxira nusxalarini yaratish tizimini yo‘lga qo‘yish kerak. Beshinchidan, kichik va o‘rta korxonalar uchun hamyonbop kiberxavfsizlik xizmatlarini rivojlantirish hamda IT mutaxassislari bilan hamkorlikni kuchaytirish taklif etiladi. Ushbu takliflarni amalga oshirish orqali korxonalarda kiberxavfsizlik darajasini oshirish, moliyaviy yo‘qotishlarni kamaytirish, mijozlar ishonchini mustahkamlash va bozordagi raqobatbardoshlikni yanada yaxshilash mumkin.

Xulosa: Men ushbu maqola ishimni yozganimdan kelib chiqqan xulosalarim bugungi kunda kiberxavfsizlik korxonalar faoliyatining muhim yo‘nalishlaridan biriga aylanib bormoqda. Raqamli texnologiyalardan foydalanish kengaygani sari korxonalarda axborotlarni himoya qilish va kiberhujumlarning oldini olish zarurati ham ortmoqda. Chunki ma’lumotlarning xavfsizligi korxonaning moliyaviy holati, mijozlar ishonchi va bozordagi obro‘siga bevosita ta’sir qiladi.Maqolani o‘rganish davomida kiberxavfsizlik st rategiyalarining korxonalar raqobatbardoshligini oshirishdagi ahamiyati ko‘rib chiqildi. Tahlillar shuni ko‘rsatadiki, zamonaviy himoya tizimlaridan foydalanish, xodimlarning bilimini oshirish va axborot xavfsizligini doimiy nazorat qilish orqali ko‘plab xavflarni kamaytirish mumkin. Shu bilan birga, bu jarayonda moliyaviy xarajatlar, malakali mutaxassislar yetishmasligi va texnologiyalarni yangilash bilan bog‘liq muammolar ham mavjud. Menimcha, har bir korxona o‘z faoliyatida kiberxavfsizlikka oddiy xarajat sifatida emas, balki kelajakdagi rivojlanishi uchun zarur bo‘lgan investitsiya sifatida qarashi kerak. Chunki mijozlar ma’lumotlarini ishonchli himoya qiladigan va zamonaviy xavfsizlik talablariga amal qiladigan korxonalar bozorda ko‘proq ishonch qozonadi. Umuman olganda, kiberxavfsizlik strategiyalarini to‘g‘ri yo‘lga qo‘yish korxonalarning barqaror faoliyat yuritishi, mijozlar ishonchini oshirishi va raqobatchilar orasida munosib o‘rin egallashiga xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonuni.
2. World Economic Forum. *Global Cybersecurity Outlook 2025*. Geneva, 2025.
3. IBM Security. *Cost of a Data Breach Report 2025*. IBM, 2025.
4. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*. International Organization for Standardization, 2022.
5. National Institute of Standards and Technology (NIST). *Cybersecurity Framework 2.0*. USA, 2024.
6. O‘zbekiston Respublikasi Kiberxavfsizlik markazi (UZCERT). Kiberxavfsizlikka oid ma’lumotlar va hisobotlar.
7. World Economic Forum. *Global Cybersecurity Outlook 2026*. Geneva, 2026.

Elektron manbalar:

- World Economic Forum – Global Cybersecurity Outlook 2025.
- IBM – Cost of a Data Breach Report 2025.
- NIST – Cybersecurity Framework.
- ISO – Information Security Management Systems