KORXONADA AXBOROT XAVFSIZLIGI TIZIMLARIGA BO‘LADIGAN HUJUMLARNI OLDINI OLISH USUL VA VOSITALAR TADQIQI

Musurmonov Behruz Farhodjon o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, talabasi

Annotatsiya: *Ushbu maqolada zamonaviy korxonalarga qarshi amalga oshiriladigan axborot xavfsizligi hujumlari va ularning oldini olish bo‘yicha nazariy hamda amaliy yondashuvlar tadqiq qilindi. Tadqiqot davomida mahalliy va xalqaro misollar, jumladan, DDoS, phishing, zararli dasturlar va ijtimoiy muhandislik hujumlari tahlil qilindi. Shuningdek, ISO/IEC 27001 va ISO/IEC 27005 standartlari asosida xavf-xatarlarni boshqarish, defense-in-depth konsepsiyasi va nol ishonch (Zero Trust) arxitekturasi kabi nazariy asoslar yoritildi. Amaliy jihatdan esa firewall, IDS/IPS, SIEM, EDR hamda XDR kabi zamonaviy texnologik vositalar samaradorligi ko‘rsatib berildi. O‘zbekiston kontekstida kiberjinoyatlar keskin o‘sayotganligi, korxonalar uchun esa xodimlarni muntazam o‘qitish va xavfsizlik siyosatlarini joriy etish zarurligi alohida ta’kidlandi. Tadqiqot natijalari shuni ko‘rsatadiki, kompleks yondashuv — ya’ni texnik vositalar, standartlashtirilgan boshqaruv tizimlari va xodimlar tayyorgarligini uyg‘unlashtirish orqali korxonalarda axborot xavfsizligi darajasi sezilarli oshirilishi mumkin.*

Abstract: *This article investigates modern cyberattacks targeting enterprises and explores both theoretical and practical approaches to their prevention. The study examines local and international cases of Distributed Denial-of-Service (DDoS), phishing, malware, and social engineering attacks. Furthermore, it highlights theoretical foundations such as risk management based on ISO/IEC 27001 and ISO/IEC 27005 standards, the defense-in-depth concept, and Zero Trust architecture. From a practical perspective, the effectiveness of technological solutions such as firewalls, IDS/IPS, SIEM, EDR, and XDR systems is discussed. The study also emphasizes the rapid growth of cybercrime in Uzbekistan, underlining the importance of continuous employee training and the implementation of strict security policies. The findings reveal that a comprehensive approach — integrating technological tools, standardized management systems, and employee preparedness — significantly enhances the level of information security within enterprises.*

Kalit so’zlar: *axborot xavfsizligi; kiber hujumlar; himoya choralari; xavf tahlili; ISO 27001.*

KIRISH

Zamonaviy korxonalarda axborot tizimlari va ma’lumot bazalari biznesning muhim qismidir. Internet va ichki tarmoqlar orqali axborot almashinuvi oshishi bilan birga korxonalarni kiberhujumlardan himoya qilish dolzarb muammoga aylandi. ISO/IEC 27001 xalqaro standarti axborot xavfsizligini boshqarish tizimlarini (ISMS) joriy etishga

qaratilgan bo‘lib, tashkilotlarga xatarlarni aniqlash, baholash va bartaraf etishda tizimli yondashuvni taklif etadi.

Ushbu maqolada korxonalarga qarshi kiberhujumlar turlari (masalan, DDoS, phishing, zararli dasturlar, ijtimoiy muhandislik), ularning oldini olish bo‘yicha nazariy yondashuvlar va amaliy texnologik yechimlar tahlil qilinadi.

Asosiy qism

Tadqiqot metodologiyasi

Maqolada adabiyotlarni sharh qilish usuli qo‘llanildi. So‘nggi yillar nashr etilgan ilmiy maqolalar, standartlar, sanoat tahlillari va ekspert hisobotlari tahlil qilindi. Xususan, ISO/IEC 27001 va ISO/IEC 27005 kabi standart hujjatlar hamda kiberxavfsizlik bo‘yicha amaliyotchi tashkilotlarning bloglari o‘rganildi. Korxonalarga qarshi hujumlar statistikasini taqdim etuvchi manbalar, jumladan kiberhujumlarga oid jahon reytinglari va O‘zbekiston kontekstidagi tahlillar ham ko‘rib chiqildi.

Korxonalarga qarshi axborot xavfsizligi hujumlari

Korxonalarni o‘tkir kiberhujumlarga nishon bo‘lishi ko‘p uchraydi. Jumladan, DDoS (Distributed Denial-of-Service) hujumlari tarmoq resurslarini ortiqcha trafik bilan to‘ldirib, xizmatdan mahrum qiladi. Bunday hujumlar jabr korxonalar serverlarini va saytlarini ishlamay qolishiga olib keladi. Misol uchun, 2023-yilda Amerika internet-provayderiga qaratilgan Mirai botneti orqali uyushtirilgan DDoS hujumi 1,4 Tbps kuchli oqimda bo‘lgani qayd etilgan.

Phishing (soxta xabarlar) – elektron pochta yoki veb-sayt orqali foydalanuvchilarning maxfiy ma’lumotlarini (login-parol, bank kartasi ma’lumotlari) firibgarlik yo‘li bilan o‘g‘irlash usuli. Masalan, hujumchi korxona xodimiga rahbar o‘rnidan soxta xabar yuborib, moliyaviy tranzaksiyalar bo‘yicha parolni so‘rab olishi mumkin. So‘nggi hisobotlarga ko‘ra, 2024-yilda respublikadagi ko‘pgina korxonalar phishing hujumiga uchragan (jahon amaliyotida BEC – Business Email Compromise) va bunday holatlarda o‘rtacha $150,000 moliyaviy zarar vujudga kelganligi qayd etilgan.

Zararli dasturlar (viruslar, troyanlar, ransomware va boshqalar) korxonalar kompyuterlariga joylab, ma’lumotlarni shifrlab yoki o‘g‘irlab zarar yetkazadi. Masalan, ransomware dasturi korxona serveridagi hujjatlarni shifrlab, ular uchun pul talabi qo‘yishi mumkin. Kiberjinoyatchilar zararli dasturlarni tarqatish uchun odatda elektron pochta ilovalari va zaif parollarni maqsad qilib oladi.

Ijtimoiy muhandislik insonga bog‘liq zaifliklardan foydalanadi: hujumchilar haqiqatga o‘xshash soxta identifikatorlar orqali xodimlarni aldab, maxfiy ma’lumotlarga kiradi. Naz et al. ma’lumotiga ko‘ra, ijtimoiy muhandislik usullari odamlarni aldash va nishon ma’lumotlarni olish san’ati bo‘lib, bu moliyaviy yo‘qotish, obro‘-e’tiborga shikast yetkazish kabi jiddiy oqibatlarga olib kelishi mumkin.

O‘zbekiston kontekstida ham kiberjinoyatchilik yuqori sur’atda o‘smoqda. Bir hisobotga ko‘ra, 2019–2024 yillarda respublikada kiberjinoyatlar soni 6700% ga oshib, jami jinoyatlar statistikasi yarmini tashkil etgan.

Korxonalarga qaratilgan hujumlar asosan moliyaviy va shaxsiy ma’lumotlarni maqsad qiladi; eng ommabop hujum vositalari sifatida zararli dasturlar va firibgarlik havolalari (60%) hamda SMS orqali ijtimoiy muhandislik (16%) qayd etilgan.

Hujumlardan saqlanishning nazariy yondashuvlari

Axborot xavfsizligini ta’minlashda birlamchi nazariy yondashuv bu – xatarlarni boshqarish (risk management). ISO/IEC 27005 standarti axborot xavfsizligi xatarlarini aniqlash, baholash va bartaraf etish bo‘yicha tuzilgan jarayonni nazarda tutadi.

Ya’ni, korxona birinchi navbatda qaysi aktivlari (ma’lumotlar, tizimlar) uchun xatar mavjudligini aniqlab, har bir xatar uchun ta’sir va ehtimolni baholaydi, so‘ngra xavflarni kamaytirishga yo‘naltirilgan choralar belgilaydi. Xavflarni oldindan aniqlab, ularga qarshi chora ko‘rish proaktiv yondashuv sifatida tizimni mustahkamlaydi.

Defense-in-depth (qatlamli himoya) konsepsiyasiga ko‘ra, bir usul yoki vosita yetarli emas, balki bir nechta himoya qatlamlarini uyg‘un ishlatish lozim.

Masalan, jismoniy himoya (kirish nazorati), texnik himoya (firewall, IDS/IPS, antivirus, šunga o‘xshash) va ma’muriy himoya (tashkilot ichidagi siyosatlar, xodimlarni o‘qitish) qatlamlari birgalikda qo‘llanadi.

Bu yondashuvda bir qatlam zaiflasa ham, boshqalar tizimni xavfdan saqlaydi. Masalan, agar hujumchi birinchi qatlamdosh logindagi zaif paroldan foydalansa, so‘ngi qatlamdagi multifaktorli autentifikatsiya (MFA) bu hujumni to‘sib qo‘yishi mumkin.

Nol ishonch arxitekturasi (Zero Trust) joriy etish ham xavfsizlikni oshiradi: bunda tarmoq perimetri ichida ham qurilmalar va foydalanuvchilarga hech qanday avtomatik ishonch berilmaydi, har bir kirish uchun alohida tekshiruv va avtorizatsiya talab qilinadi.

Bu printsipga ko‘ra korxona tarmog‘idagi har bir qurilma va foydalanuvchi faoliyati uzluksiz tekshiriladi, bu esa ma’lumotlar buzilishini sezilarli darajada kamaytiradi.

O‘rnatilgan siyosatlar va standartlar ham muhim. Masalan, ISO/IEC 27001 standarti xavf-xatarlarni boshqarishning majburiy talablari va ISMSni takomillashtirish jarayonlarini belgilaydi.

Ushbu standartni qo‘llagan tashkilotlar ma’lumotlar xavfsizligini risk nuqtai nazaridan boshqarib, kamchiliklarni proaktiv tarzda bartaraf etish imkoniyatiga ega bo‘ladi. Muntazam audit va xavfsizlik tekshiruvlari («penetratsiya testi» va boshqa sinovlar) ham tizimdagi zaif joylarni aniqlashga yordam beradi.

Amaliy yechimlar: vositalar, tizimlar va texnologiyalar

Korxonani himoya qilishning amaliy choralari bir nechta turkumga bo‘linadi. Tarmoq himoyasi uchun firewall, router va xavfsizlik devor tizimlari (masalan, WAF – Web Application Firewall) qo‘llanadi. Shuningdek, IDS/IPS (buzilishlarni aniqlash/oldini olish) tizimlari tarmoq trafiki va tizim xatti-harakatlarini kuzatib, g‘arazli harakatlarni aniqlaydi. Keng tarqalgan xavfli trafikni aniqlash va yo‘naltirish uchun CAPTCHA, DDoS himoyasi yoki botlarni boshqarish vositalari ham ishlatiladi.

Endpoint xavfsizligi uchun esa kompyuterlarga va serverlarga o‘rnatiladigan EDR (Endpoint Detection and Response) va klassik antivirus/antimalware yechimlari zarur. Ular zararli dasturlarni real vaqtda aniqlab, zararlanishga qarshi choralarni ishga

tushiradi. Ma’lumotlarni himoya qilish uchun DLP (Data Loss Prevention) tizimlari korxona tashqarisiga maxfiy ma’lumotlarning chiqishini nazorat qiladi. Shu bilan birga, ma’lumotlar bazalari va xotirani shifrlash (encrypt) orqali ruxsatsiz foydalanishdan saqlanish mumkin.

Xavfsizlik ma’lumotlarini tahlil qilish uchun SIEM (Security Information and Event Management) tizimlari qo‘llaniladi. SIEM xavfsizlik voqealari loglarini birlashtiradi, voqealarning ketma-ketligidan anomaliyalarni aniqlashga yordam beradi. Yangi avlod yechimlari — XDR (Extended Detection and Response) platformalari — esa tarmoq, chekka qurilmalar va bulut xizmatlaridagi ma’lumotlarni to‘plab, ularni kross-kanalli tarzda tahlil qiladi, bu orqali tahdidni to‘liq kontekstdan ko‘rib chiquvchi keng qamrovli himoyani ta’minlaydi.

Kiruvchi va chiquvchi trafikni filtrlash uchun xavfsiz kirish servislari (SASE, CASB) ham keng tarqalgan. Masalan, Secure Access Service Edge (SASE) orqali korxona ob’ektiga bog‘langan barcha qurilmalar bulut asosidagi xavfsizlik qatlamlari orqali nazorat qilinadi. Shuningdek, ko‘p omilli autentifikatsiya (MFA) joriy etish orqali foydalanuvchilarni paroldan tashqari qo‘shimcha mexanizmlar bilan tekshirish amalga oshiriladi.

Oxirgi, lekin muhim qism — xodimlarni o‘qitish va huquqiy chora-tadbirlar. Texnik vositalardan tashqari, foydalanuvchilarni kiberhujumlardan ogohlantirish, odatda phishing’ga qarshi simulyatsiya o‘tkazish va xavfsizlik bo‘yicha treninglar tashkil qilish orqali inson omili zaifligi kamaytiriladi. Shuningdek, korxona ichida axborot siyosati, xavfsizlik me’yorlari va ISO/IEC 27001 talablariga mos hujjatlari ishlab chiqilgan bo‘lishi lozim. Bugungi kunda O‘zbekistonda ham kompaniyalarga axborot xavfsizligi bo‘yicha majburiy talablar kuchaytirilmoqda, moliyaviy va hukumati tashkilotlar bunday talablar ostida ishlamoqda.

Xulosa

Korxonalarda axborot xavfsizligini ta’minlash bo‘yicha samarali himoya strategiyasi bir nechta qatlamdan tashkil topishi kerak: texnik vositalar, siyosatlar va xodimlar tayyorligidan iborat bo‘lishi zarur. Zamonaviy tahdidlardan samarali himoya qilish uchun ISO/IEC 27001 kabi xalqaro standartga mos yondashuv, xavf-xatarlarni boshqarish jarayonlari va defense-in-depth printsiplari qo‘llanilishi muhim ahamiyatga ega.

Ya’ni, firewall va IDS dan tortib EDR va SIEMgacha bo‘lgan vositalar birgalikda ishlab, kiruvchi trafikni filtrlash, zararli dasturlarni aniqlash va tarmoqlarni segmentlash orqali birinchi chiziq himoyasini yaratadi.

Xodimlarni doimiy ravishda himoya siyosatlari va AML (O‘qitish, xabardorlik) dasturlari bilan ta’minlash ijtimoiy muhandislik hujumlariga qarshi himoyani kuchaytiradi.

Xulosa qilib aytganda, axborot xavfsizligini ta’minlash tizimli va kompleks choralar talab qiladi. Zamonaviy texnologiyalar (AI/ML asosidagi tahdidlarni aniqlash, Zero Trust, XDR kabi) va xalqaro xavfsizlik yondashuvlari birgalikda korxona ma’lumotlarini samarali himoya qilish imkonini beradi.

Standartlar bo‘yicha ISMSni joriy etish esa tashkilotlarga xavf-xatarlarni sistematik boshqarish, uzluksiz audit va doimiy takomillashtirishni olib borishga yordam beradi.

ADABIYOTLAR RO’YXATI:

1. Biplob, M.B., Marma, S., & Akther, M. (2024). Securing Tomorrow’s Digital World: Key Trends in Cyber security for 2024. Preprints. doi:10.20944/preprints202409.0576.v1

2. Naz, A., Sarwar, M., Kaleem, M., Mushtaq, M.A., & Rashid, S. (2024). A comprehensive survey on social engineering-based attacks on social networks. International Journal of Advanced and Applied Sciences, 11(4), 139–154.

3. International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 – Information security management systems – Requirements. Geneva, Switzerland: ISO.

4. International Organization for Standardization (ISO). (2022). ISO/IEC 27005:2022 – Guidance on managing information security risks. Geneva, Switzerland: ISO.

5. Cloudflare, Inc. (n.d.). What is “defense in depth”?. Cloudflare Learning Center. Retrieved from https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth/

6. Special Eurasia. (2025, June 3). Rising Cybercrime Alarms Uzbekistan’s National Security. Retrieved from https://www.specialeurasia.com/2025/06/03/cybercrimes-uzbekistans/

7. Hoxhunt. (2025). Phishing Trends Report (Updated for 2025).