KOMPYUTER TARMOG‘IDA IQTISODIY AXBOROTLAR XAVFSIZLIGINI TA’MINLASH

Ernazarov Alisher Ergashevich,
Samarqand iqtisodiyot va servis instituti dotsenti
Berdiqulova Madina Zokir qizi,
Samarqand iqtisodiyot va servis instituti talabasi

Annotatsiya: Ushbu maqolada axborot resurslari va kompyuter tarmog’ida iqtisodiy axborotlar xavfsizligini ta’minlash chora-tadbirlari yoritib berilgan. Shuningdek, iqtisodiy axborotlarni ularga qilinadigan kiber-hujumlardan himoya qiluvchi dasturlardan foydalanishni joriy etish ko’zda tutilgan.

Kalit so’zlar: axborotlar xavfsizligi, himoyalash texnologiyalari, tahdid, raqamli imzo, Kriptografiya

Abstract: This article describes measures to ensure the security of information resources and economic information in the computer network. It is also planned to introduce the use of programs that protect economic information from cyber-attacks.

Key words: information security, protection technologies, threat, digital signature, Cryptography

Аннотация: В данной статье описаны меры по обеспечению безопасности информационных ресурсов и экономической информации в компьютерной сети. Также планируется внедрить использование программ, защищающих экономическую информацию от кибератак.

Ключевые слова: информационная безопасность, технологии защиты, угрозы, электронная подпись, криптография.

Hozirgi kunda kompyuter tarmoqlari iqtisodiy sohada katta rol o'ynaydi. Ko'pgina muhim axborot jarayonlari tarmoq tizimlari orqali amalga oshiriladi va ularning faoliyatining muvaffaqiyati ularning xavfsizligiga bog'liq. Kompyuter

tarmog'idagi iqtisodiy ma'lumotlar jiddiy xavfsizlikni talab qiladigan maxsus toifadagi ma'lumotlardir. Bunday ma'lumotlar buxgalteriya hisobi, moliyaviy ma'lumotlar, xalqaro shartnoma muzokaralari va raqobatchilar yoki hujumchilar uchun qimmatli bo'lishi mumkin bo'lgan boshqa materiallarni o'z ichiga olishi mumkin. Kompyuter tarmog'ida iqtisodiy axborot xavfsizligini ta'minlash uchun kompleks yondashuvni qo'llash kerak.

Ma’lumki, yildan-yilga texnika-texnologiyalar va sun’iy intellektlarning rivojlanishi natijasida iqtisodiy axborotlar xavfsizligini ta’minlash chora-tadbirlarini ishlab chiqish masalasiga katta e’tibor qaratila boshladi. Avvalambor, axborotlar xavfsizligi tushunchasiga e’tibor beradigan bo’lsak, bu fuqarolar, tashkilotlar va davlat manfaati yo’lida jamiyat axborot muhitini shakllantirish, takomillashtirish hamda undan foydalanish jarayonlarida uning ichki va tashqi tahdidlardan himoyalanganligini ta’minlovchi holatdir. Shunga ko’ra, axborot xavfsizligining konseptual modelini axborot manbalari, axborotga kirish usullari, tahdid, tahdid manbalari, tahdid obyektlari, himoya usullari, himoya vositalari, himoya yo’nalishlaridan iborat ekanligini ko’rishimiz mumkin.

Hisoblash vositalari va axborot uzatish tizimlarining jadal rivojlantirish bilan bir qatorda ularning xavfsizligini ta’minlash muammosi tobora dolzarb tus olmoqda. Xavfsizlik choralari axborotlarni ruxsatsiz olish, himoya qilinayotgan axborotlarni yo’q qilishning oldini olishga qaratilgan. Yuqorida keltirilgan xavflarning kelib chiqishini tasodifiy, oldindan ko’zda tutilgan yoki qasddan qilingan deb aytishimiz mumkin. Tasodifiy xavflar dasturiy ta’minlshdagi xatolar, apparat vositalarining ishdan chiqishi, foydalanuvchi yoki ma’muriyatning noto’g’ri harakatlari oqibatida yuzaga kelishi mumkin. Qasddan qilingan tahdidlarda foydalanuvchilarga zarar yetkazish maqsadi mavjud bo’lib, unga quyidagilar kiradi: 1) konfendentsial axborotlarni oshkor qilish; 2) axborot resurslaridan ruxsatsiz foydalanish; 3) axborot resurslaridan noto’g’ri foydalanish; 4) axborotlarni ruxsatsiz almashtirish; 5) axborotlarni rad etish; 5) xizmat ko’rsatishdagi rad etish.

Bundan tashqari, hozirgi paytda kompyuter viruslari ham axborotlar xavfsizligiga salbiy ta'sir ko'rsatadi. Ularning turlari haddan ortiq ko'pligi sababli bu viruslarga qarshi ishonchli himoya vositalarini ishlab muammosi asosiyligicha qolmoqda. Iqtisodiy axborotlar tizmidagi axborotlarni ishlab chiqishda tijorat siri bo'lgan ma'lumotlarni, shuningdek, kompyuterlardagi axborot tizimining o'zida ham xavfsizlik bo'yicha muammolar kelib chiqadi.

Yuqorida keltirilgan muammolarning oldini olishning, ya'ni axborotlarni himoyalashning eng samarali usullari kiptografik usullar yig'inisi hisoblanib, "kiptografiya" so'zi "sirli yozuv" degan ma'noni anglatadi va u axborotlarning o'zaro ta'siri jarayonida ularni himoyalash usullarini o'rganadi. Bunda shifrlash mexanizmidan foydalaniladi. Yuborishga tayyor axborotlar, u ma'lumot bo'ladimi, nutq yoki birorta hujjatning jadval ko'rinishidagi tasviri bo'ladimi, odatda, ular xabar deb ataladi. Bunday xabarlarni aloqaning himoyalanmagan kanallari bo'yicha yuborish jarayonida ular yashirincha tinglaydigan shaxsning qasddan yoki shunchaki eshitishi vositasida osongina to'xtatib qolinishi yoki kuzatilishi mumkin. Bu ma'lumotlarga ruxsatsiz kirishning oldini olish uchun u shifrlanadi va shu bilan shifrogramma yoki yashirin matnga aylanadi. Ruxsat etilgan foydalanuvchi ma'lumotni olgach, uni yechadi yoki qaytadan o'zgartirilgan kriptogramma vositasida olingan dastlabki matn shakliga keltirib, o'qiydi. Kriptografiya tizimida qayta o'zgartirish usuliga maxssu algoritmdan foydalanish mos keladi. Bunday algoritmning harakati noyob son yoki shifrlaydigan kalit deb ataladigan izchillik natijasida yuborilishi bilan amalga oshiriladi. Foydalaniladigan har bir kalit faqat shu kalit bilan belgilanadigan turlicha shifrlangan xabarlarni o'tkazadi. Ko'pchilik uchun kalit generatori chizmasini yopiq tizimi yoki qism apparatura uzellari (kardware), yohud kompyuter dasturi (software) yig'indisi yoki ularning hammasini birgaligi sifatida ko'rinishi mumkin. Biroq har qanday holatda ham shifrlash/shifrni ochish jarayoni yagona tarzda, tanlab olingan maxsus kalit bilan aniqlanadi. Shu bois, shifrlangan xabarlarni almashish yuboruvchi uchun ham, oluvchi uchun ham muvaffaqiyatli o'tishi uchun kaditni to'g'ri o'rnatishni

bilish va uni sir saqlash zarur. Shifrlash simmetrik va asimmetrik bo'lishi mumkin. Simmetrik shifrlash bitta maxfiy kalit shifrlash va uni "ochish"da qo'llanilishiga asoslanadi. Asimetrikda esa shifrlashda hamma bop bitta kalitdan, uni "ochish"la esa boshqa shu bilan umumiy kalit bilish uni imkonini bermaydigan "maxfiy" kalitdan foydalanilishi bilan tavsiflanadi.

Shifrlash bilan bir qatorda xavfsizlikning boshqa mexanizmlaridan ham foydalaniladi. Masalan: raqamli elektron imzo; kirish huquqining nazorati; ma'lumotlarning yaxlit butunligini ta'minlash; autentifikatsiya bilan ta'minlash; jadval o'rnatish; yo'naltirishni boshqarish; tekshiruvdan o'tkazish.

Raqamli imzo maxanizmlari asimmetrik shifrlashning algoritmlariga asoslanadi va bajariladigan ikki ish tartibiga ega: yuboruvchining imzosoni shakllantirish va oluvchining uni topib olishi (verifikatsiya). Birinchi ish tartibi ma'lumotlar blokini shifrlash yoki uni kriptografik nazorat miqdori bilan to'ldirishini ta'minlaydigan, shu bilan birga ikkala holatda ham jo'natuvchining maxfiy kalitidan foydalaniladi. Ikkinchi ish tartibi esa jo'natuvchining tanib olishi uchun bilishi yetarli bo'lgan hammabop kalitdan foydalanishga asoslanadi.

Dasturlashtirilgan vositalar o'zida axborotlarni himoyalash vazifasini bajrish uchun dasturlashtirilgan ta'minotni aks ettiradi.

Himoyalashning tashkiliy vositalari o'zida axborotlarni himoyalashni ta'minlash uchun hisoblash texnikalarini, telekommunikatsiya apparaturalarni tayyorlash va ishga tushurish jarayonida amalga oshiriladigan tashkiliy – texnik va tashkiliy – huquqiy chora – tadbirlarni aks ettiradi. Tashkiliy chora – tadbirlar apparaturalarning, hayotiy davri bosqichlaridagi hamma bosqichlari qurulmaviy elementlarini qamrab oladi.

Kompyuter tarmog'ida iqtisodiy axborot xavfsizligini ta'minlash ruxsatsiz kirish, ma'lumotlarning sizib chiqishi va kiberhujumlarning oldini olishning muhim jihati hisoblanadi. Kompyuter tarmog'idagi iqtisodiy ma'lumotlarning xavfsizligini ta'minlash uchun quyidagi qadamlar qo'yilishi mumkin:

1. Kuchli parollardan foydalaning: Harflar, raqamlar va maxsus belgilar kombinatsiyasidan iborat kuchli parollardan foydalaning. Parollarni muntazam ravishda o'zgartiring va barcha hisoblar uchun bir xil paroldan foydalanmang.

2. Ko'p faktorli autentifikatsiya: Hisoblaringiz uchun ko'p faktorli autentifikatsiyani yoqing. Mobil telefonga kod yuborish kabi qo'shimcha tekshirish darajasi ruxsatsiz kirishning oldini olishga yordam beradi.

3. Dasturiy ta'minotni yangilash: Topilgan zaifliklarni tuzatish uchun barcha dasturiy ta'minot va operatsion tizimlarni muntazam yangilab turing.

4. Xavfsiz ulanishdan foydalaning: Veb-saytlarga kirishda har doim HTTPS kabi xavfsiz ulanishdan foydalaning. Bu uzatilgan ma'lumotni ushlashdan himoya qilishga yordam beradi.

5. Xavfsizlik devori va antivirus: Buzg'unchilarning oldini olish va zararli dasturlarni aniqlash uchun tarmoqdagi barcha kompyuterlarga xavfsizlik devori va antivirus dasturlarini o'rnating.

6. Kirish cheklovi: Kompyuter tarmog'iga kirishni faqat vakolatli foydalanuvchilar uchun cheklash. Kirish huquqlarini boshqarish uchun turli kirish darajalaridan foydalaning.

7. Xodimlarni muntazam ravishda o'qitish: xodimlaringizni potentsial tahdidlardan xabardor bo'lishlari va xavfsizlikni saqlash uchun tegishli choralarni ko'rishlari uchun ularni axborot xavfsizligi asoslariga o'rgating.

8. Ma'lumotlarni zahiralash: muntazam ravishda barcha muhim ma'lumotlaringizni zaxiralang va xavfsiz joyda saqlang. Bu muammo yuzaga kelganda ma'lumotni tiklashga yordam beradi.

9. Tarmoq faoliyatini monitoring qilish: Har qanday noodatiy faoliyat yoki ruxsatsiz kirish urinishlarini aniqlash uchun tarmoq faolligini monitoring qilish tizimlarini o'rnating.

10. Xavfsizlik siyosatini yaratish: kompyuter tarmog'ida iqtisodiy axborot xavfsizligini ta'minlash qoidalari va tartiblarini belgilovchi xavfsizlik siyosatini ishlab chiqish va amalga oshirish.

Yuqorida keltirilgan barcha tahdidlar, nafaqat, iqtisodiy axborotlar, balki barcha turdagi ma’lumotlar va shaxsiy axborotlar uchun ham o’rinli bo’lib, ularni himoyalashda samarali metodlardan foydalanish muhim hisoblanadi. Shuningdek, bularni amalga oshirishning eng foydali va ommabop yo’li kriptografiya(shifrlash)ni tatbiq etish maqsadga muvofiqdir.

Shuni ta'kidlash kerakki, kompyuter tarmog'idagi iqtisodiy axborot xavfsizligi doimiy e'tibor va himoya usullarini yangilashni talab qiladi. Hujumchilar doimiy ravishda ma'lumotlarni buzish va ma'lumotlarga kirishning yangi usullarini topmoqdalar, shuning uchun kompaniyalar axborot xavfsizligi sohasidagi so'nggi ishlanmalarni kuzatishi va xavfsizlikning eng yangi usullarini qo'llashi kerak.

Xulosa qilib aytadigan bo'lsak, kompyuter tarmog'ida iqtisodiy axborot xavfsizligini ta'minlash kompaniyaning muvaffaqiyatli va xavfsiz ishlashining ajralmas qismidir. Integratsiyalashgan yondashuv va zamonaviy xavfsizlik usullaridan foydalanish xavflarni minimallashtirish va ma'lumotlar xavfsizligini ta'minlashga yordam beradi.

Foydalanilgan adabiyotlar:

1. Аксенова Г.М. Информационная безопасность организации. - М.: Питер, 2016.
2. Батуев А.А. Безопасность компьютерных систем и сетей. - М.: Эксмо, 2014.
3. Васильев А.Б. Безопасность информационных технологий. - М.: Изд-во "Юрайт", 2020.
4. Ergashevich, E. A. (2023). PRACTICAL APPLICATION OF INNOVATIVE TECHNOLOGIES IN THE HIGHER EDUCATION SYSTEM. *Journal of Advanced Scientific Research (ISSN: 0976-9595)*, *3*(2).
5. Turakulov, O., & Ernazarov, A. (2023). TALABALARNING INTELLEKTUAL QOBILIYATLARINI RIVOJLANTIRISH

USULLARI. *Евразийский журнал социальных наук, философии и культуры*, *3*(11), 70-75.

6. Ergashevich, E. A. (2023). ANALYSIS OF THE STATE OF USE OF MODERN TEACHING METHODS AND TECHNOLOGIES IN EDUCATIONAL INSTITUTIONS. *Journal of marketing, business and management*, *2*(6), 7-12.
7. Ergashevich, E. A. (2023). Some Pedagogical Technologies Used in the Process of Organizing Training Sessions in Higher Education Institutions. *Information Horizons: American Journal of Library and Information Science Innovation (2993-2777)*, *1*(9), 14-19.