DOI: https://doi.org/10.5281/zenodo.12216753

KORPORATIV AXBOROT TAHDIDLARI VA HIMOYALASH DARAJALARI

Sayfullayev Sherzod Baxtiyor o‘g‘li
Axborot xavfsizligi kafedrasi doktoranti,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Ganiyev Abduxalil Abdujalilovich
Axborot xavfsizligi kafedrasi dotsenti
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: *Mazkur maqolada koporativ axborotga bo‘ladigan tahdidlar va korporativ axborotdan himoyalanish darajalari, xususan, ma’muriy, huquqiy-me’yoriy, kriptografik hamda dasturiy-texnik to‘siqlar tadqiq qilingan.*

Kalit so‘zlar: *korporativ axborot, tahdid, .himoya, ruxsatsiz foydalanish.*

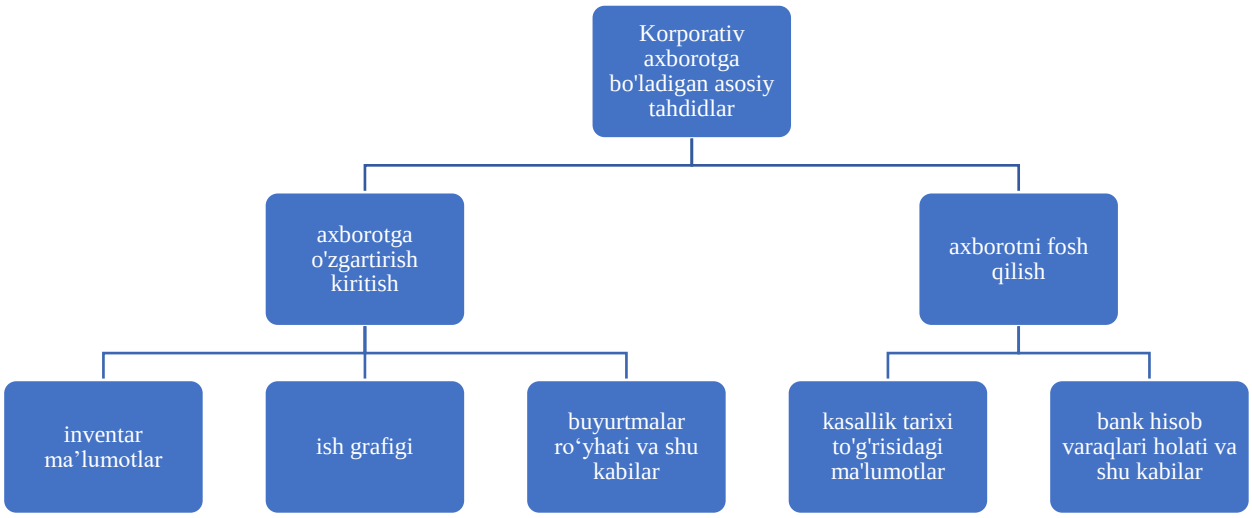
Korporativ axborotni himoya qilish zarurati strategik sohalarda tadqiqotlarning maxfiyligini ta’minlash, sanoat ishlanmalari to‘g‘risidagi ma’lumotlarni to‘g‘ri taqsimlash va zamonaviy jamiyatda shaxs to‘g‘risidagi shakllanishning intensivligini tartibga solish zarurati bilan bog‘liq. 80-yillarning boshlari demokratik mamlakatlardagi ijtimoiy noroziliklar global xakerlar tarmog‘ini birlashtirishga yordam bergan boshlang‘ich nuqta sifatida qaraladi. Inson huquqlarining buzilishi asosida dunyoning bir qator mamlakatlarida deyarli bir vaqtning o‘zida ko'plab buzg‘unchilik tashkilotlari paydo bo‘ldi. Bir yildan kamroq vaqt o‘tgach, ushbu guruhlar muvaffaqiyatli hamkorlik qila boshlashdi. Ularning a‘zolari milliy chegaralar bo‘ylab ko‘pincha o‘g‘irlangan parol orqali telefon tarmog‘iga bepul kirish orqali erkin o‘zaro g‘oyalar almashinuvini yo‘lga qo‘yishdi.

Ma’lumotlarni himoya qilish muammolari maxfiy va shaxsga doir ma’lumotlarni qayta ishlash va saqlash uchun kompyuterlardan foydalanganda yaqqol namoyon bo‘ladi. Ma’lumotlarni himoya qilish bo‘yicha umumiy chora-tadbirlar majmuini o‘rnatmasdan, ularni shifrlash yetarli bo‘lmaydi. Kompyuterda saqlangan ma‘lumotlar uchun qanday tahdidlar paydo bo‘lishi mumkinligini hamda havaskor va buzg‘unchilar tomonidan ruxsatsiz foydalanish natijasida qanday yo‘qotishlar ro‘y bo‘lishi mumkinligi quyida ko‘rib chiqiladi.

Korporativ axborot tahdidlari. Eng umumiy holatda tahdidlarning faqat ikki turi mavjud: axborotni fosh qilish va o‘zgartirish. Korporativ axborotni oshkor qilish deganda, kimdir tasodifan yoki maqsadli harakatlardan keyin ma‘lumotlarning ma’nosi ma’lum bo‘lishi tushuniladi. Ushbu turdagi buzilish eng keng tarqalgan hisoblanadi. Oqibatlari turlicha bo‘lishi mumkin. Fosh etilishidan ehtiyotkorlik bilan himoyalangan o‘ta muhim ma’lumotlar shaxsga doir ma'lumotlardir: kasallik tarixi, xatlar, bank hisob varaqlari holati va shu kabilar.

Biroq, ko‘plab mutaxassislarning fikriga ko‘ra, kompyuterlarning joriy qilinishi bilan shaxsga tahdidlar kompyuterlardan keng foydalanishgacha bo‘lgan davrdagi darajada va bir xil holatda qoldi.

Korporativ axborotni oshkor qilishdan kelib chiqadigan yo‘qotish turlari quyida ko‘rib chiqiladi. Odatda, shaxsga doir ma‘lumotlar o‘z egalari uchun juda muhim, ammo o‘g‘rilar uchun unchalik ahamiyatga ega emas. Ba‘zida shaxsga doir ma'lumotlar nafaqat shaxslarni, balki butun tashkilotlarni buzish uchun ham ishlatilishi mumkin. Ammo buni amalga oshirish uchun qat’iy axloqiy asosga ega bo‘lmagan holda murosaga kelgan kishi, aksariyat hollarda, ko‘proq narsa yo‘qotadi. Biroq, shaxsga doir ma‘lumot o‘z-o‘zidan qimmatli, uni oshkor qilishning asosiy zarari insonning o‘ziga baxtsizlik olib keladi. Ammo strategik boshqaruv ma‘lumotlarini oshkor qilish katta ahamiyatga ega. Agar ishlab chiqarishni rivojlantirishning uzoq muddatli rejasi yoki bozordagi vaziyatni tahlil qilish to‘g‘risidagi axborot fosh qilinsa, unda ushbu ma‘lumotga egalik qiluvchi uchun bu yo‘qotishlar sezilarsiz bo‘ladi, ammo raqobatchilar uchun bunday ma‘lumotlar juda muhimdir. Ma‘lumotdan ruxsatsiz foydalanish juda keng tarqalgan bo‘lsa-da, kamdan-kam hollarda jiddiy zarar keltiradi, chunki u ko‘pincha g‘arazli niyatda amalga oshirilmaydi, ya’ni, tasodifan yoki qiziquvchanlik tufayli.

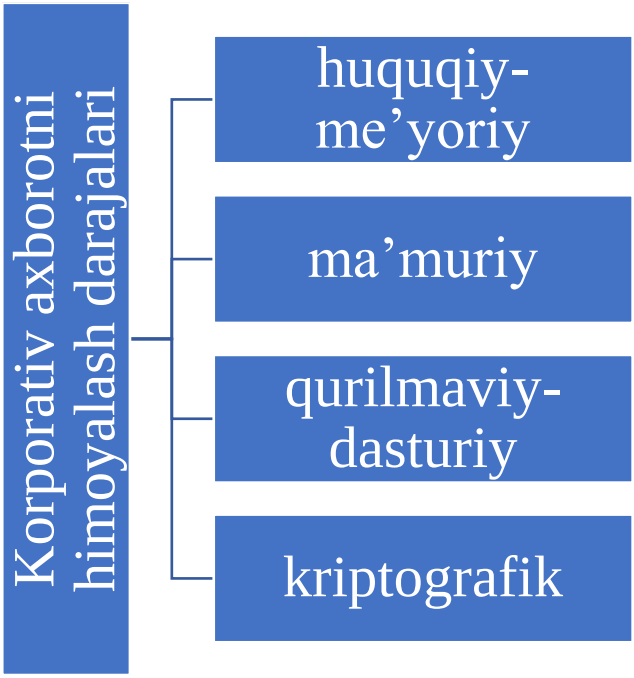


1-rasm. Korporativ axborotga bo’ladigan asosiy tahdidlar va tahdid uchraydigan axborotlar

Axborotni buzilishi sezilarli darajada katta xavfni hosil qiladi. Ko‘plab tashkilotlarda juda muhim ma’lumotlar fayllar ko‘rinishida saqlanadi: inventar ma’lumotlar, ish grafigi, buyurtmalar ro‘yhati. Agarda bunday ma’lumotlar o‘zgartirilsa yoki o‘chirib yuborilsa, faoliyat bir qancha vaqtga to‘xtab qolishi mumkin. Eng xavfli tomoni shundaki, sodda kriptografik tizimlarda bunday o‘zgartirishlarni amalga oshirish uchun kalitni ham bilish shart emas. Shu sababli qat’iy shifrlar nafaqat axborotni fosh bo‘lishidan, balkim birlik bitni sezilmasdan o‘zgartirilishiga ham bardoshlilikni ta’minlanishini kafolatlashi lozim. Ma’lumki, yo‘qotilishi juda katta zararlarga olib keladigan iqtisodiy xarakterdagi axborotlar o‘zgartirishlarga eng zaif hisoblanadi. Bu toifadagi kompyuter jinoyati sababli to‘g‘ridan-to‘g‘ri ulkan moliyaviy yo‘qotishlarni olib kelishi mumkin. Katta ilmiy va dasturiy loyiha rahbarlari ma’lumotlar katta xavfni raqobatchilar emas, balki o‘z xodimlari hosil qiladi. Turli sabablarga ko‘ra xodimlar yakuniy loyihani o‘zgartirib yuborishi yoki umuman yo‘q qilib yuborishi ham mumkin. Bunday kutilmagan hodisalar IBM korxonasida ro‘y bergan. Avstraliyaga buyurtma qilingan dasturiy tizim olib kelingan. Dastlabki muvaffaqiyatli sinovdan so‘ng, ishga tushirish jarayonida tizim nosoz holatga kelgan. Tergov jarayonidan keyin ma’lum bo‘lishicha, bir dasturchi sinov jarayonida o‘z dasturida xatolikni aniqlagan va sirli holda qo‘riqlanadigan tizim nusxasiga tuzatish kiritgan. Boshqa dasturlar tomonidan bu xatolik tuzatilganidan bexabar bo‘lgan dasturchining ikki karra tuzatishi IBM korxonasiga bir necha million dollarga tushish mumkin edi. Shunday qilib, favqulodda

muhim ma’lumotlar shifrlangan shaklda saqlanishi yoki buzilishni istisno qilish uchun hech bo‘lmaganda raqamli imzo bilan tasdiqlanishi lozim [1].

Korporativ axborotni himoyalash darajalari. Ruxsatsiz foydalanish toifasidagi hujumlar amalga oshirilish ehtimoli mavjud ma’lumotlar himoya ostida bo‘ladi. Ulardan ruxsatsiz foydalanishga erishish uchun ketma-ketlikda to‘rt to‘siqni, to‘rt himoya darajasini buzib o‘tish talab etiladi. Quyida bu darajalar batafsil ko‘rib chiqiladi.



2-rasm. Korporativ axborotni himoyalash darajalari (to’siqlar)

Korporativ axborotdan ruxsatsiz foydalanishni amalag oshirishda inson oldida turadigan birinchi to‘siq – huquqiy-me’yoriy to‘siq. Bu axborotni himoayalash bo‘g‘ini axborotni uzatish hamda qayta ishlashda etik va yuridik me’yorlarga rioya qilish bilan bog‘liq. Baxtga qarshi, qonunchilikning mukammal emasligi hamda uning keng targ‘ib etilishi, uni turlicha talqin etilishiga olib keladi, bu esa axborotdan ruxstasiz foydalanishga bo‘lgan asoslarni (va asoslanishlarni) ro‘yhatini kengaytiradi.

Zamonaviy kompyuter buzg‘unchiligi bilan kurashda katta to‘siq bo‘lib xalqaro bo‘linish xizmat qiladi. Kompyuter buzg‘unchiligi odatda milliy chegalarni kesib o‘tadi. Bu xalqaro o‘lchovlar kompyuter buzg‘unchilariga qarshi samarali kurashda katta yuridik to‘siq hosil qiladi. Ichki kompyuter buzg‘unchiligida bunday toifadagi muammolar mavjud emas va yuridik jihatdan oddiy jinoyatdan farq qilmaydi. Biroq agarda kompyuter jinoyatchilik joyi xorijda yoki shubhali shaxs boshqa mamlakatdan turib jinoyatni amalga oshirgan bo‘lsa, unda suverenitetning an’anaviy konsepsiyasi milliy jinoiy huquq va yurisdiksiyani qo‘llashni qat’iy cheklaydi [2].

Korporativ axborotdan ruxsatsiz foydalanishda oldinda paydo bo‘ladigan ikkinchi to‘siq ma’muriy to‘siq. Huquqiy me’yorlar va ijtimoiy bo‘g‘inlarni hisobga olgan holda barcha toifadagi rahbarlar kim va qanday axborotni saqlashi hamda yig‘ishi, shaxsga axborotdan foydalanish huquq hamda majburiyatlari va tarqatish yo‘llarini boshqarish va boshqaga berishni belgilaydi. Umuman rahbariyatning ko‘plab yechimlari mahalliy organlarning farmonlari va qonunlari hamda siyosatdan kelib cihqib belgilanadi, biroq ko‘plab muammolar tashkilot ichkarisida ma’muriyat istaganidek hal qilinadi. Tizim ma’muriy himoyasini ta’sirli choralari amalga oshirilmaguncha boshqa choralar samarasiz bo‘ladi. Ma’muriy choralarni amaliy tarzda amalga oshirish asosan tizimga va unda qayta ishlanuvchi axborotga insonlarni ruxsatini cheklash bilan realizatsiya qilinadi. Axborotni himoylashning tashkiliy choralari etik choralarga nisbatan unchalik muhim hisoblanmaydi, dasturiy va texnik choralarga nisbatan esa noaniq va samarasi kam hisoblanadi. Biroq bu axborotdan noqonuniy foydalanish va boshqa darajalar uchun asos bo‘lishda kuchli to‘siq bo‘la oladi, ya’ni ma’lumotlarni bank kompyuteridan nusxalab olish, universitet kompyuteridan ma’lumotni nusxalashdan sezilarli darajada murakkabroq bo‘ladi.

Ikkinchi to‘siqning muhimligini hisobga olgan holda uni amalga oshirish muammolariga batafsilroq to‘xtaladi. Samarali ma’muriy choralarni hayotga tadbiq qilish murakkabligining sabablaridan biri axborotni himoyalash nisbatan yangi va oddiy vazifa emasligi to‘g‘risidagi fikr-mulohazalarning mavjudligidir. Biroq ma’lumotni himoyalash har doim va hamma joyda mavjud bo‘lgan, faqatgina axborot tizimlari bo‘lmaganda boshqacharoq amalga oshirilgan. Endi jamiyat axborot sanoatiga aylandi. Axborot tizimlarining tezkorligi va bajaruvchanligi oldingi davrda bo‘lmagan vaziyatlarni vujudga kelishi uchun zamin yaratdi. Himoyaning tashkiliy choralarini kiritishdagi boshqa muammo uning amalga oshirilishi foydalanuvchilarga noqulayliklarni yuzaga chiqarishidadir. Bunda istalgan ma’muriy choralari xodimlarda ularning fuqarolik huquqlarini cheklanayotgandek hamda avvalgi ish haqi evaziga qo‘shimcha ish bajarilishi talab etiladigandek hissiyot uyg‘otadi. Deyarli barcha rahbarlar hisoblashi bo‘yicha shaxsiy javobgarliksiz aybdorlarni topish ilojsiz va bu shunday ham aslida.

Uchinchi himoya darajasi – qurilmaviy-dasturiy daraja. Bu foydalanuvchiga ma’lumotlar va dasturiy vositalarga ruxsatni ochuvchi foydalanuvchi identifikatsiyasidan iborat. Qurilmaviy himoya kodli karta, navbatchi bilan savol-javob tarzidagi ma’lumot almashinuvi, kalitlar va jetonlar tarzida amalga oshirilishi mumkin. Buning samaradorligi kuchli shubha tug‘diradi. Hozirgi adabiyotlarda qurilmaviy himoya bo‘yicha individual kartalar, parollar, ovoz va elektrom izmo identifikatsiyasi tavsiflanadi, biroq bularning barchasi yoki qimmat, yoki yetarlicha ishonchli emas. Bunday turdagi himoya tizim ma’lumotlaridan ruxsatsiz foydalanishdan ogohlantira

ola olmagan. Bundan tashqari qurilmaviy himoyani zaifligi – insonlardir. Ular ishda qulayliklar yaratishni yoqtirishmaydi.

Oxirgi to‘rtinchi himoya darajasi – kriptografik himoyadir. Ma’lumotlar ma’nosini yashirish maqsadida ularni shifrlashni nazarda tutiladi. Foydalanuvchi kalit bo‘yicha identifikatsiya jarayonidan muvaffaqiyatli o‘tmaguncha, ma’lumot ma’nosi mavhum bo‘ladi. Ma’lumotlar bu holda xabar deb ko‘riladi va ularni ma’nosini himoyasi uchun shifrlashni klassik texnikasidan foydalaniladi. Kriptografiya uch komponentani bo‘lishini nazarda tutadi: ma’lumotlar, kalit va kriptografik tizim. Shifrlashda joriy ma’lumot xabar hisoblanib, natijaviy ma’lumot esa shifr bo‘ladi. Deshifrlash jarayonida ular joy almashinadi.

Kriptografik algoritm barcha uchun ochiq, biroq foydalanuvchi xabar ma’nosini yashirish uchun foydalangan kalitni bilmasdan xabar matnini qayta tiklashga juda katta mehnat talab etiladi. Aytib o‘tish joziki, buzilishga to‘liq bardoshli shifrlash mavjyd emas. Shifr sifati faqatgina uni buzish uchun ketadigan moliyaviy xarajat miqdorigagina bog‘liq. Bunday talab zamonaviy kriptografik tizim bilan qoniqtiriladi, masalan, “AQSh milliy standartlar byurosining ma’lumotlarni shifrlash standarti” bo‘yicha yaratilgan AES. Ba’zi toifadagi ma’lumotlarning buzilishi o‘ta xavfli bo‘lganligi va buni konteksdan aniqlash murakkabligi sababli, odatda istalagn simvolni o‘zgarishiga sezgir bo‘lgan shifrlash usullari foydalaniladi. Bu nafaqat yuqori maxfiylikni biroq, xatoliklar yoki istalgan buzlishni samarali aniqlashni ham kafolatlaydi.

Cheklovlar o‘rnatmasdan ma’lumotlardan ruxsatsiz foydalanishga qarshi choralarni baholashdan oldin himoya darajalari bo‘yicha xulosa chiqariladi.

Xulosa qilib aytganda, kompyuter buzg‘unchiligi faoliyatining turli yo‘nalishlarini qonunchilik bilan birgalikda ko‘rib chiqish natijasida shunday xulosaga kelish mumkinki, zamonaviy huquqiy tizimning ortda qolayotganini hamda mukammal emasligi ayon bo‘ladi. Qonunchilik hozirgi bosqichda ko‘rib chiqilayotgan xavfli harakatlar uchun javobgarlikka tortish (jinoiy javobgarlikka ham) imkoniyatiga ega.

Foydalanilgan adabiyotlar ro‘yxati

1. Holmstrom B., Kaplan S.N. The state of US corporate governance: What’s right and what’s wrong. Journal of Applied Corporate Finance, 2003, no. 15, pp. 8–20.

2. Kelly L. The Development of a Positive Theory of Corporate Management’s Role in External Reporting. Journal of Accounting Literature, 1983 (Spring), pp. 111–150.