DOI: https://doi.org/10.5281/zenodo.11245408

HUJUM MANBALARI VA SABABLARI

Ramazonova Madina Shavkatovna
Ilmiy rahbar

Tojimuratov Shuxratbek Dilmurodjon o‘g‘li
Mirzayev Bekzod Toxirboy o‘g‘li
Babajanov Jaloliddin Umidjon o‘g‘li
Toshkent axborot texnologiyalar universiteti talabalari
abdujabbor.madina.1989@gmail.com

Annotatsiya: *Bu maqola axborot tizimlarining ishlashida chet elda chetda ishlatilayotgan qo‘shimcha xavfsizlikni ta’minlash masalasiga bag‘ishlangan. Bu xavfsizlik muammolari qaysi sabablarga asoslangan, ularning oqibatlari, va ularni bartaraf etishning texnik va insiyativ usullari maqolada ta’riflangan.*

Kalit so‘zlar: *Axborot tizimlari, Xavfsizlik, Buzg‘unchilik,Xodimlar, Ijtimoiy choralar, Foydalanuvchilar*

Axborot xavfsizligi tizimini ishlab chiqishda buzg‘unchilikka kim yoki nima sabab bo‘lishi mumkinligini, bu tasodifiymi yoki qasddan qilingan harakatmi, uni takrorlash mumkinmi, ayrim hollarda oqibatlarini bartaraf etishning qanday mexanizmlari mavjudligini aniq tushunish kerak.

Axborot tizimlarining ishlashidagi uzilishlarning eng keng tarqalgan sababi bu foydalanuvchilarning xatolari, tashkilot xodimlarining tasodifiy xatolari bo‘lib, bu odatda katta zararga olib kelmaydi, biroq istisnolar bo‘lishi mumkin.

Bunday nosozliklarning o‘ziga xos xususiyati barcha tomonlarning bunday vaziyatlarning yuzaga kelishiga yo‘l qo‘ymaslik va yetkazilgan zararni minimallashtirish istagidir. Natijada, xatoga yo‘l qo‘ygan xodimga, agar holatni yashirgan bo‘lsa, unga nisbatan ma’muriy jazo qo‘llash tavsiya etiladi. Bunday xatolarning asosiy aybdorlari biznes-texnologlar va tizimni ishlab chiquvchilardir. Zamonaviy nazorat va monitoring mexanizmlari bu toifadagi buzg‘unchiliklarni deyarli butunlay bartaraf etish imkonini beradi. Biroq, xatolar turlarining ko‘pligi sababli, ularning paydo bo‘lishini butunlay yo‘q qiladigan tizimni yaratish odatda mumkin emas yoki asossiz xarajatlar bilan bog‘liq.

Keling, xodimlarning tasodifiy xatolarini ko‘rib chiqaylik. Axborot tizimlari bilan bog‘liq inson xatolarining 80% dan ortig‘ini kiritish xatolari tashkil qiladi. Charchoq, turli shovqinlar, o‘qib bo‘lmaydigan yozuvlar - bularning barchasi ma’lumotlarni qo‘lda kiritishdagi xatolarga olib kelishi mumkin. Bunday xatolarning aksariyati asosiy xususiyatga ega emas, ammo noto‘g‘ri miqdor yoki noto‘g‘ri tafsilotlarni kiritish kabi xatolar jiddiy oqibatlarga olib kelishi mumkin. Qo‘lda kiritish xatolariga qarshi kurashning asosiy vositalari uni avtomatlashtirish va elektron hujjat aylanish tizimlarini ishlab chiqishdir. Bunday yechimning imkoniyatlari tugagan taqdirda quyidagi mexanizmlar qo‘llaniladi:

– katalog bo‘yicha asosiy parametrlarni nazorat qilish;

– hujjatlarni ikki marta kiritish; shablonlardan foydalanish; xodimlarning ish yukini kamaytirish;

– hujjatni qo‘shimcha vizual nazorat qilish.

Tizimni ishlatishdagi xatolar tizim bilan ishlaydigan xodimlarning tajribasi yetarli emasligi bilan bog‘liq.

Ko‘pincha, bu turdagi xatolik yangi axborot tizimlarini joriy qilishda yoki mavjudlarining funksionalligini o‘zgartirishda yuzaga keladi. Xodimlarning mas’uliyati o‘zgarganda yoki yangi xodimlar ishga qabul qilinganda ham kutilishi kerak bo‘lgan bunday xatolarning oldini olish uchun, odatda, foydalanuvchilarning noto‘g‘ri harakatlari ehtimolini oldini olish uchun tashkilotda yaxshiroq o‘qitish tizimlari va huquqlarni cheklashning aniq tizimi qo‘llaniladi.

Tizimlashtirish xatolari turli ob’yektlarni noto‘g‘ri tasniflash bilan bog‘liq (masalan, uni ochishda noto‘g‘ri huquqni belgilash). Bunday xatolar juda kam uchraydi va odatda jiddiy yo‘qotishlarga olib kelmaydi. Ularning eng ehtimoliy oqibati - hisobotlardagi xatolar yoki hujjatlarni qayta ishlashdagi xatolardir. Buning sababi asosan bilim va tajribaning yetishmasligi va ularni bartaraf etish qiymati, asosan, axborot tizimining moslashuvchanligi va ularni aniqlash tezligiga bog‘liq bo‘ladi. Qaror qabul qilish jarayonini avtomatlashtirish yoki mumkin bo‘lgan qiymatlar oralig‘ini cheklaydigan avtomatlashtirilgan filtrlar xatolardan himoya qilishi mumkin, ammo o‘zgaruvchan muhitda ushbu mexanizmlarni qo‘llab-quvvatlash juda qimmatga tushishi mumkinligini yodda tutish kerak.

Beparvolik, texnologik zanjirning buzilishi. Afsuski, xodimlarning o‘z vazifalarini bajarishga beparvo munosabati bilan bog‘liq xatolar ko‘p uchraydi. Qoidabuzarlikning ushbu guruhi jazo tizimini ishlab chiqishni talab qiladigan, qasddan sodir bo‘lmagan xatolarning yagona hisoblanadi. Biroq, ushbu guruhning noaniqligini hisobga olish kerak. Xodim ishda charchaganmi yoki mas’uliyatsizmi, buni baholash juda qiyin.

Keling, xodimlarning qasddan harakatlarini, oldini olish eng qiyin bo‘lgan buzg‘unchilikni ko‘rib chiqaylik. Tashkilot xodimi, odatda, ichki jarayonlar va tizimlarni yaxshi biladi. Ko‘pincha u xavfsizlik mexanizmlari va, eng xavflisi, ma’lum tizim modullarida ularning yo‘qligi haqida biladi. U o‘z harakatlarini modellashtirish va sinab ko‘rish va oqibatlarini baholash uchun vaqt va imkoniyatga ega.

Xodimlarning qasddan harakatlariga qarshi xavfsizlik tizimining yana bir zaif nuqtasi tashkilotning boshqa xodimlarining ularga bo‘lgan ishonchidir.

Ko‘pincha, ma’murga shaxsiy ma’lumotlarga kirish uchun oddiy so‘rov yoki ishlab chiquvchidan ba’zi xavfsiz ko‘rinadigan tizim funksiyasini qo‘shish so‘rovi, keyinchalik undan noqonuniy harakatlar uchun foydalanish uchun yetarli.

Xodimlarni axborot xavfsizligini ataylab buzishga undaydigan sabablar quyidagilardir:

– odatda nizolar yoki xodimni ishdan bo‘shatish bilan bog‘liq bo‘lgan menejerlarning harakatlariga nisbatan norozilik;

– qo‘shimcha pul ishlashga harakat qilish;

– tashkilotdan pul o‘g‘irlashga urinish;

– tashkilotning ma’lum bir xodimga qaramligini yaratishga urinish: martaba kurashi.

Ushbu turdagi buzg‘unchiliklarga qarshi kurashning eng samarali choralari ijtimoiy choralar, kirishni nazorat qilish va foydalanuvchi harakatlarini kuzatishdir.

Axborot tizimlarining ishlashidagi buzilishlarning sabablari uchinchi shaxslarning jinoiy xarakterdagi harakatlari ham bo‘lishi mumkin. Matbuot va kinoda ushbu mavzuga e’tibor kuchayib borayotganiga qaramay, real zarar keltirgan bunday buzg‘unchiliklar soni kamaygandan ko‘ra ortib bormoqda. Ehtimol, bu aynan ushbu qonunbuzarliklarning haddan tashqari reklamasi tufayli yuzaga kelgandir va natijada axborot texnologiyalari sohasidagi maksimal mablag‘ ulardan himoyalanish uchun sarflanadi. Biroq, shuni tan olish kerakki, kredit tashkilotlari haqiqatan ham diqqat markazida.

Jinoyatchilar, odatda, bitta maqsadga ega – bu pul, unga erishish usullari esa doimiy ravishda takomillashtirilmoqda. Shuning uchun, potensial buzilishlarni tahlil qilganda, mumkin bo‘lgan hujum ob’yektlarini aniqlash kerak. Avvalo, bular masofaviy to‘lov tizimlari, xususan, plastik kartalar yordamida amlaga oshiriladigan to‘lov tizimlari. Hujum muvaffaqiyatli tugasa, jinoyatchi jazosiz qolish uchun ko‘p imkoniyatlarga ega.

Hujumning yana bir maqsadi bank ma’lumotlar ombori bo‘lishi mumkin, keyinchalik ularni nashr qilish bilan shantaj qilinadi.

Noqonuniy xatti-harakatlarning uchinchi varianti, ularni bartaraf etish bo‘yicha o‘z xizmatlarini taklif etish maqsadida kredit tashkilotining axborot tizimining

ishlashiga aralashish bo‘lishi mumkin. Qoidaga ko‘ra, bunday urinishlar osongina fosh qilinadi, shuning uchun bunday buzg‘unchilik juda kam uchraydi va axborot xavfsizligi xizmatlari bozorida o‘z nomiga ega bo‘lmagan kompaniyalar tomonidan qo‘llaniladi.

Buzg‘unchilar tahdidlarining yana biri - o‘zgartirilgan tizim komponentlarini joriy etish (buni bank xodimlarining hamkorligisiz amalga oshirish deyarli mumkin emas), bu katta mablag‘larning o‘g‘irlanishiga olib kelishi mumkin.

Hujumchilar yaxlitlash algoritmlariga o‘z o‘zgartirishlarini kiritgan va butun balansni o‘z hisoblariga o‘tkazgan holatlar haqida hamma biladi. Bunday hujumlarga qarshi yagona himoya ishlatiladigan algoritmlarning doimiy auditi va avtomatik ravishda aniqlangan miqdorlarni parallel ravishda mustaqil nazorat qilish bo‘lishi mumkin.

Yuqorida keltirilgan misollar barcha mumkin bo‘lgan holatlarni qamrab olmaydi. Doimiy ravishda pul mablag‘larini o‘g‘irlashning yangi usullarini o‘ylab topishga urinayotgan jinoyatchilarga qarshi turish axborot xavfsizligi tizimining eng muhim vazifasidir.

Keyingi bo‘lishi mumkin bo‘lgan sabab - bu raqobatchilarning faoliyati. Bank biznesining qonunlari adolatli raqobatni talab qilishiga qaramay, raqobatchilar bilan noqonuniy kurashish uchun axborot texnologiyalaridan foydalanish mavjud. Bu yerda axborot xavfsizligi tizimiga hujum qilishning ikkita variantini ko‘rib chiqish mumkin.

Birinchi variantning maqsadi shunchaki ma’lumotlarni yig‘ishdir: mijozlar, operatsiyalar va bozor haqida. Odatda bularning barchasi bank xodimlaridan ba’zi ma’lumotlarni sotib olishga urinish bilan bog‘liq. Ko‘pincha, ular orasida vijdonsiz shaxslar ma’lumotni raqobatchilarga sotishga harakat qilishadi. Bunga turli xil ijtimoiy choralar, shuningdek, bunday ma’lumotlarni sotishga urinayotgan boshqa tashkilotlar xodimlarining shunga o‘xshash faoliyatini bostirish orqali qarshi turish mumkin.

Ikkinchi variantda, raqobatchi axborot tizimiga kirishdan bevosita manfaatdor bo‘ladi. Bank biznesida buning uchun katta resurslarni jalb qilish mumkin. O‘rta menejerlar darajasida bunday hujumga qarshi turish deyarli mumkin emas.

Va nihoyat, oxirgi sabab - baxtsiz hodisalar, tabiiy ofatlar va boshqa tasodifiy hodisalar.

Tasodifiy hodisalardan himoya qilishning asosiy muammosi - ularning oldindan aytib bo‘lmaydiganligi va xavf darajasini hisoblash metodologiyasining yo‘qligi. Bunday hodisalarning past ehtimoli oqibatlarning yuqori narxi bilan qoplanadi. Ko‘pincha tasodifiy hodisalar (yong‘in, tabiiy ofat yoki oddiy quvur yorilishi) axborot tizimining to‘liq yo‘q qilinishiga olib keladi va tashkilotning vazifasi hatto ekstremal holatlarda ishni davomiyligini saqlab qolishdir, ham menejer bunday holatlar uchun qanday asosiy himoya usullarini borligini bilishi va ulardan foydalanishi talab etiladi.

Xalqaro amaliyot tashkilotning mavjud byudjetiga qarab bir nechta himoya choralarini tavsiya qiladi. Ular asosan tizimni zaxira nusxalash bilan bog‘liq. Bularga quyidagilar kiradi:

– ko‘p tarmoqli tashkilotlar uchun - bir-birining hududida turli bo‘linmalarning o‘zaro zaxira nusxalarini yaratish. Favqulodda vaziyatlarda ma’lumotlar tiklanadi va bir bo‘linma hududi boshqasiga zaxira ofis sifatida ishlatilishi mumkin;

– katta byudjetga ega tashkilotlar uchun - zaxira ofisini yaratish. Odatda, u asosiy tashkilotning bazaviy funktsiyalarini nusxalaydi va tashkilotning faqat favqulodda rejimda ishlashini ta’minlaydi. Buning uchun bitta server, ikki yoki uchta xona va tashqi axborot tizimlariga chiqish bo‘lishi kifoya. Voqea sodir bo‘lgan taqdirda, zaxira idorasi tashkilotning ishlashini bir haftadan ko‘p bo‘lmagan vaqtda ta’minlashi kerak. Shu vaqt ichida asosiy ofisni tiklash yoki yangisini ijaraga olish masalasi hal qilinishi kerak;

– Cheklangan byudjetga ega bo‘lgan tashkilotlar uchun axborot tizimining har kuni zaxira nusxasini yaratish va nusxalarini boshqa hududda saqlash tavsiya etiladi. Bu do‘stona tuzilma yoki arxivni saqlash xizmatlarini ko‘rsatadigan ixtisoslashgan kompaniya bo‘lishi mumkin.

Xulosa: Bu maqola axborot tizimlarining ishlashida uzoq muddatli xavfsizlik muammolariga oid holatlar, sabablar va bartaraf etish usullarini taqdim etadi. Xavfsizlik muammolari foydalanuvchilar, xodimlar, tizimlashtirish xatolari va jinoyatchilar tomonidan yuzaga kelishi mumkin. Maqolada uning asosiy sabablari va ularni bartaraf etishning imkoniyatlari ta’riflangan. Taqdim etilgan ma’lumotlar xavfsizlik sohasidagi ko‘p tomondan ta’sirchan masalalarni ko‘rib chiqishda yordam berishi mumkin.

ADABIYOTLAR

1. O‘zbekiston Respublikasi Konstitutsiyasi.

2. O‘zbekiston Respublikasi Fuqarolik kodeksi. 01.03.1997. Qayta taxrirlangan versiyasi (21.04.2022y).

3. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. 16.04.2019 y.

4. O‘zbekiston Respublikasining «Axborot olish kafolatlari va erkinligi to‘g‘risida» Qonuni. 24.04.1997 y.

5. Yevropa Kengashining 1981 yil 28 yanvardagi “Shaxsiy ma’lumotlarni avtomatik qayta ishlash bo‘yicha jismoniy shaxslarni himoya qilish to‘g‘risida”gi konventsiyasi. Elektron resurs: lexdigital.ru/2012/052/ (Murojaat sanasi: 12.11.2015).

6. Yevropa Parlamenti va Kengashning 1996 yil 11 martdagi “Ma’lumotlar bazalarini huquqiy himoya qilish to‘g‘risida”gi 96/6/EC direktivasi. Elektron resurs

7. Yevropa Parlamentining 2001 yil 22 maydagi “Axborot jamiyatida mualliflik huquqi va turdosh huquqlarning ayrim jihatlarini uyg‘unlashtirish to‘g‘risida”gi 2001/29/EC direktivasi. Elektron resurs: http://www. wipo.int/wipolex/ru /text.jsp?file_id=126976 (Murojaat sanasi: 09.12.2015).

8. 2000 yil 8 iyundagi 2000/31/EC-sonli “Ichki bozorda axborot xizmatlarining ayrim huquqiy jihatlari to‘g‘risida”gi Yevropa Ittifoqi Direktivasi №2000/31/EC. Elektron resurs: http://www.wipo.int/wipolex/ru/text.jsp? file_id=181678 (Murojaat sanasi: 15.10.2015).

9. 1996 yil 20 dekabrdagi “BIMTning Mualliflik huquqi to‘g‘risida”gi Shartnomasi. - Jeneva: BIMT. – 2000. - № 226(R).

10. A.Sokolov, O.Stepanyuk. Защита от компьютерного терроризма. O‘quv qo‘llanma. BXV-Peterburg. Arlit, 2002.