IQRO JURNALI / 2023
GUVOHNOMA № 060680
E-ISSN : 2181-4341
https://wordlyknowledge.uz
IMPACT FACTOR(SJIF) : 3,934
Volume 3 issue 2 - 2023

AXBOROT-KOMMUNIKATSIYA TARMOQLARIDA TARMOQ XAVFSIZLIGINI BOSHQARISHNING AHAMIYATI

Gulrukh Matkurbanova Alisher qizi
O'zbekiston jurnalistika va ommaviy kommunikatsiyalar universiteti
Fakultet: Oliy jurnalistika kurslari magistratura

Annotatsiya
Maqolada axborot-kommunikatsiya tarmoqlari av ijtimoiy tarmoqlarda tarmoq xavfsizligini boshqarish va ushbu jarayonda kompleks kuzatuv markazlarini qurish usullari va vositalari haqida umumiy malumot berilgan bo'lib soha olimlarining zamonaviy tadqiqot va tahlillari natijasiga ko'ra bazi xulosa va takliflar keltirilgan.
Kalit so'zlar:
Ijtimoiy tarmoqlar, internet, kiyberxavfsizlik, axborot xurujlari, boshqaruv markazlari, tarmoq xavfsizligi, protocol, sertifikatlash.

KIRISH

Bugungi kunda inson shunchaki bitta tugmani bosish orqali e-mail, audio yoki video orqali har qanday ma'lumotni uzatish yoki qabul qilish imkoniyatiga yega, lekin ma'lumotni qay darajada xavfsiz almashilinmoqda yoki boshqa insonga axborot qanchalik xavfsiz yetib borayotganligi haqida hech o'ylab ko'rganmikan? Bu savolning javobi kiber xavfsizlikda yotadi. Hozirda internet har kunlik hayotning eng tez o'sayotgan infratuzilmasidir. Hozirgi texnika dunyosida eng so'nggi texnologiyalar inson yashash tarzini o'zgartirib yubormoqda. Lekin yangi chiqayotgan texnologiyalar tufayli biz axborotimizni eng samarali yo'l bilan ham xavfsiz saqlay olmaymiz va shuning uchun kiber jinoyatlar kundan-kunga ko'payib bormoqda. Hozirda 60% dan ortiq moliyaviy kelishuvlar internet orqali amalga oshiriladi, shuning uchun bu soha kata miqdordagi kelishuvlar uchun eng yaxshi sifatli xavfsizlikni talab qiladi. Kiber xavfsizlikning ko'lami faqatgina axborot texnologiyalari sanoatida axborotni himoyalash yemas, balki kibermakon kabi boshqa ko'pgina turlarga bo'linadi.

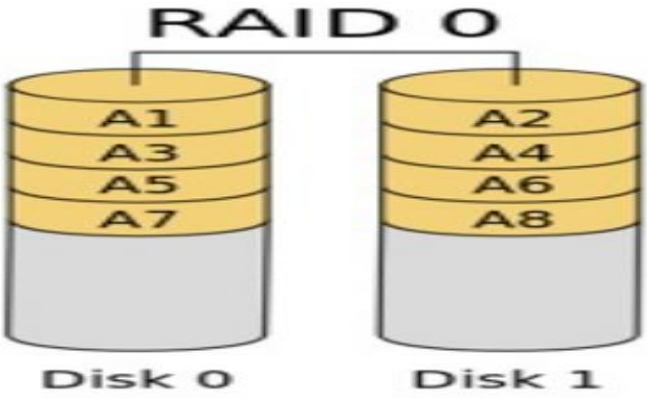
Ma'lumki, barchani qiziqtirayot gan axborotlarni dastlabki shakllari ma'lumotlar bazalarida saqlanadi, ya'ni kompyuterning disk qurilmalarida joylashgan bo'ladi. Aynan shu qurilmadagi ma'lumotlar bazalarini tashqi ta'sirlardan saqlay olish eng asosiy masalalardan hisoblanadi, chunki bundagi axborotni buzilishi nafaqat tashqi ta'sir, bevosita ichki ta'sirdan bo'lish ehtimoli ham mavjud.

Albatta tarmoq xavfsizligi masalasiga to'xtalishdan oldin umumiy kiber xavfsizlik tushunchasi, kompyuterning ichkli axborot palatasi va unga aloqador bazi dasturiy paketlar haqida so'z yuritish maqsadga muvofiqdir.

Kiber xavfsizlik. Ma'lumotlarni maxfiyligi va xavfsizligi har bir tashkilot himoya qiladigan asosiy xafvsizlik choralari hisoblanadi. Biz har qanday ma'lumot kiber yoki onlayn shaklda saqlanadigan dunyoda yashayapmiz. Ijtimoiy tarmoqlar bizni oilamiz va do'stlarimiz bilan xafvsiz muloqot qila oladigan saytlar bilan ta'minlaydi. Bu holda kiber jinoyatchilar ijtimoiy tarmoqlarni insonlarning shaxsiy ma'lumotlarini o'g'irlashda va foydalanishda davom yetadilar. Nafaqat ijtimoiy tarmoqlarda, balki bank kelishuvlarida ham barcha xavfsizlik choralari ko'rilishi lozim[1].

[1] Dilmurod Raxmatov "Kiber jinoyatlarni yuzaga kelish omillari va kiber etika: muammo va istiqbollar" "Science and Education" Scientific Journal Volume 1 Issue 1 230-b

Ko‘p yillik kuzatuv natijalarida shu ma’lum bo‘ldiki, magnit golovkasini disk yuzasi bo‘ylab uzoq muddatda suzib yurishi(o‘qish, yozish ishlari) vaqtlar o‘tishi bilan ko‘pincha magnit xossalarini pasayib diskdagi axborotni o‘chishiga, ishdan chiqishiga olib keladi. Bunday holatda diskdagi axborotni doimo o‘chmasdan, kompyuterni to‘xtovsiz ish rejimini ta’minlab beradigan tizimni shakllantirish va uning yordamida ishlarni to‘xtovsiz ishlab turishlik talab etiladi. Bunday tizim qatoriga RAID (redundant array of independent disks, inglizcha-bir-biriga bog‘liq bo‘lmagan disklarning to‘liq massivi ma’nosini anglatadi) ni kiritish mumkin.
RAID tushunchasida, ma’lumotlarni virtuallashtirish texnologiyasi tamoyilida bir necha disklarni mantiqiy birlashtirish orqali axborot massivini o‘chmasdan turishligini ta’minlash orqali ish unumdorligini oshirishdan iborat. Demak, RAID usuli orqali massiv o‘chmasligi ta’minlanadi va ish to‘xtamaydi. RAIDning birnecha turlari mavjud: RAID0, RAID1, RAID2, RAID3 va boshqa turlari. Bu turlar(daraja)dagi massivlarni saqlanishida o‘ziga xos yutuqlar va kamchiliklar mavjud. Bularni alohida-alohida ko‘rib chiqamiz va sharhlaymiz[2].



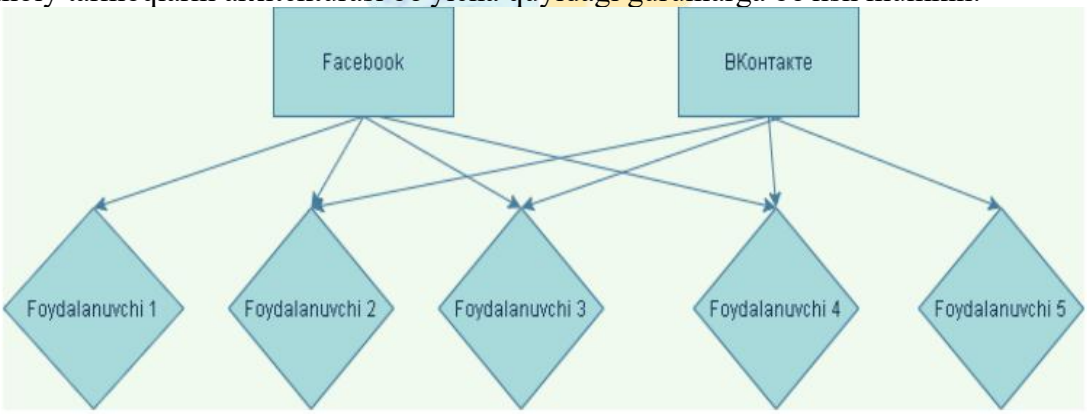
1-rasm. Nosozlikka chidamli yuqori unumda ishlovchi disk massivi.

RAID0 usulini «Nosozlikka chidamli yuqori unumda ishlovchi disk massivi» deb ham yuritiladi (1-rasm). RAID0 ning boshqalardan farqi unumliligidadir, lekin bu massivning himoyalanish darajasi past , broq quyidagi afzalliklari mavjud:
— kat ta hajmdagi ma’lumotlarni qayta ishlash va kiritish-chiqarish so‘rovlarini amalga oshirish talablarida yuqori unumni namoyon etishi;
-bu usulni qo‘llashda soddalik;
— massivni hosil qilishda mablag‘ni kam sarf bo‘lishligi. Shular bilan bir qatorda quyidagi kamchiliklar mavjud:
— to‘xtovsiz ish unumini ta’minlash imkoniyatini yo‘qligi;
RAID 1 usulini «Ko‘zguli yoki zaxiralangan disk massivi» deb ham nomlanadi. Bu usulda «Mirroring», ya’ni, ikkita diskning ko‘zguli aksi yoki soyasi shakllantiriladi. Ushbu massivlarning qo‘shimcha "soya«lari uni yuqori ish unumdorligi bilan ishlashini ta’minlaydi. «Soya» lar ortiqcha xarajatlarni yuzaga keltirib, massivni qayta ishlashdagi tannarxni oshishiga olib keladi.— bit ta diskdagi ma’lumotni o‘chib qolishi boshqa disklardagi barcha disklarni o‘chib ketishiga olib kelishi bilan farqlanadi.
Agar xodimlar tarkibida axborot xavfsizligi bo'yicha yaxshi mutaxassislarga ega bo'lgan tashkilotlar biron bir himoyaga ega bo'lsa, unda ma'lumotlar uzatish tarmoqlarining oddiy foydalanuvchisi xavfsizlik jarayonidagi eng himoyalanmagan bo'g'in hisoblanadi.
Ko'pincha ular trolling, kashchenizm yoki kiberhujumlarning turli xil turlari qurbonlari bo’ladi. Afsuski, maxsus ma'lumotga ega bo'lmagan yoki biron bir kompyuter mahoratiga ega bo'lmagan

[2] Белая книга. ЗАЩИТА ДАННЫХ XTREMIO (XDP). Защита данных на флэш — дисках в массивах XtremIO. Апрель 2015 г. 2015 Корпоратsія EMC.(https://www.emc.com/kk-kz/index.htm)

oddiy foydalanuvchi Internet axborot xavfsizligi tahdidlarining himoyasiz qurboniga aylanadi. Shuning uchun ular ko'pincha kiberjinoyatchilarning qurboniga aylanishlari ajablanarli emas. Hujum tashkilotga qaratilgan bo'lsa ham, foydalanuvchi baribir qurbon bo'ladi. Axborot-kommunikatsiya tizimlarida ijtimoiy tarmoqlar tuzilishini tahlil qilish. Ijtimoiy tarmoq deganda grafigi sifatida aks ettirilishi mumkin bo'lgan tugunlar to'plami (foydalanuvchilar, guruhlar yoki jamoalar) va ular orasidagi bog'lanishlar (ijtimoiy o'zaro aloqalar) dan iborat bo'lgan tuzilma tushuniladi.

Ijtimoiy tarmoqlarni arxitekturasi bo'yicha quyidagi guruhlarga bo'lish mumkin:



2-rasm. Ijtimoiy tarmoqlarning markazlashtirilgan arxitekturasi

Qisman markazlashtirilmagan (gibrid) yechimlar (2-rasm). Birgina misol bu ko'plab o'zaro bog'langan tugunlardan tashkil topgan Diaspora ijtimoiy tarmog'i, ularning har biri alohida veb-server. Ijtimoiy tarmoq mijoz-server arxitekturasiga ega, foydalanuvchilar ulanadigan serverni tanlashlari mumkin.

Shunday qilib, biz xulosaga kelishimiz mumkinki, agar ijtimoiy tarmoqlarda buzg'unchi ma'lumotlarning tarqalishini to'xtatish zarur bo'lsa, foydalanuvchilarning butun ijtimoiy tarmoqni to'liq blokirovka qilish kerak bo'lmasdan tarqalishi va o'zaro aloqasi amalga oshiriladigan bir nechta tugunlarni blokirovka qilish kifoya.

XULOSA VA MULOHAZALAR

Xulosa o’rnida shularni ayta olamizki mamlakatimizda axborot tarmoqlari xavfsizligi asta sekin umumjahon darajasiga ko’tarilmoqda albatta ushbu sohada xalqaro rivojlanish darajasi bo’yicha hali yuqori o’rinda emasmiz. Bu ayni haqiqat.

Xorijiy axborot xavfsizligi markazlari Internetda keng namoyish etiladi. Faoliyatining ustuvor yo‘nalishlariga ko‘ra, bunday markazlar ajralib turadi.

ADABIYOTLAR

1. В.И. Завгородний Комплексная защита информатsии в компьютерных системах. (Учебное пособие). М.: Изд. «Логос»., 2001.—261 с.
2. R.H.KUSHATOV “Axborot xavfsizligi va intellektual mulkka kirishni boshqarish” O‘quv qo‘llanma Samarqand – 2021 132-b
3. Xashimov Sabit xan Kompyuter tarmog‘idan foydalanishda axborot xavfsizligi muammolari va ularni hal etish usullari” Евразийский научный журнал 332-b
4. C. Xashimov, To‘xtasinov M., Mag.Abdullaeva S. Mahalla yoshlari tomonidan sodir etilayot gan xuquqbuzarliklarni oldini olishda kompyuter texnologiyalaridan foydalanish muammolari.Informatika va energetika muammolari, O‘zb.jurnali, 4-son, 2008, 66-72 b.
5. P.Karimov, M.Dadamirzaev Mahalla faoliyatini boshqarishda axborot-kommunikatsiya texnologiyalaridan foydalanish. Toshkent axborot texnologiyalari universit yet ining 60-yillik

yubileyiga bag‘ishlangan «Radiotexnika, telekommunikatsiya va axborot texnologiyalari: muammolari va kelajak rivoji» mavzusidagi xalqaro ilmiy-texnik konferensiyasi maqolalar to‘plami, 1-tom,Toshkent 2015 yil 21-22 may,571-575-betlar.
6. Рашидов, Д. (2023). Давлат-хусусий шерикликда таваккалчилик турлари. *Scienceweb academic papers collection*.
7. Белая книга. ЗАЩИТА ДАННЫХ XTREMIO (XDP). Защита данных на флэш-дисках в массивах XtremIO. Апрель 2015 г. 2015 Корпоratsiя EMC.(https://www.emc.com/kk-kz/index.htm)
8. Cyberleninka.ru
9. Google.com
10. Elektronhujjat.uz

WORDLY
KNOWLEDGE