OPTIK ALOQA TARMOQLARIGA QARATILGAN ICHKI VA TASHQI TAHDIDLAR

Ashurov Azizbek Ergash o‘g‘li,
Ziyamatova Saodat Xasanovna,
Karimova Nafisa Po‘lat qizi
Toshkent shahar Shayxontohur tumanidagi Kasb hunar maktabi informatika o‘qituvchilari

Annotatsiya: Ushbu maqolada optik aloqa tarmoqlarida ichki va tashqi tahdidlarga qarshi zamonaviy usullardan foydalangan holda kiberxavfsizligini ta’minlash, dasturiy va apparat-dasturiy vositalari tahlil qilingan.

Kalit so‘zlar: optik aloqa, internet, kiberxavfsizlik, tahdid, himoya, dastur, TriplePlay, CompTIA.

KIRISH

Optik aloqa tarmoqlari ko‘p jihatdan boshqa tarmoqlarga nisbatan afzalliklarga ega bo‘lsada, xavfsizlik masalalarida ular ham yetarli darajada muammolarga ega.

Keng polosali ulanish xizmatlarini amalga oshirish uchun optik tolali texnologiyalarni joriy etish (masalan, TriplePlay va boshqalar), elektron hujjat aylanishiga o‘tish va buning natijasida kompaniyaning axborot xavfsizligiga yangi tahdidlarning sezilarli darajada oshishi, tashqi va ichki qoidabuzarlar tashkilotlar rahbariyatidan ushbu xavf-xatarlarni samarali bartaraf eta oladigan choralar ko‘rishni talab qiladi. Shu bilan birga, hozirgacha O‘zbekistonda ham, boshqa davlatlarning milliy darajasida ham optik tolali aloqalar orqali axborotni sizib chiqishidan himoya qilish sohasida himoya vositalari yetarli emas va bu muammo ustida izlanishlar olib borilmoqda.

ASOSIY QISM

Optik tarmoqlar muhim ijtimoiy xizmatlarni qo‘llab-quvvatlovchi va katta hajmdagi ma’lumotlarni tashuvchi muhim infratuzilmani ifodalaydi. Bunday aloqa infratuzilmalari xizmatlarini buzishga qaratilgan hujumlarning asosiy nishoni hisoblanadi. Optik qatlamda ma’lumotlar xavfsizligini ta’minlash past kechikishli ma’lumotlarni shifrlashni ta’minlaydi va xavfsiz ma’lumotlarni uzatish imkoniyatlarini oshiradi. Xavfsiz va yuqori tezlikda uzatishga bo‘lgan talab keskin ortib borayotganligi sababli, xavfsiz ma’lumotlarni uzatish qayta ishlash tezligi va tarmoq sig‘imi talablarini kuchaytirmoqda. Optik tolali tizimlar aloqa tarmoqlarining

asosini tashkil etganligi sababli, tarmoq xavfsizligini himoya qilish uchun optik yondashuvlar tarmoqning mavjud sig‘imini oshiradi. Bundan tashqari, elektr zanjirlari bilan solishtirganda, optik tolali tizimlar elektromagnit shovqinlarga qarshi bardoshli va yuqori ishlov berish tezligiga ega.

Optik aloqa tarmoqlarida xavfsizlikning ikki ko‘rinishini farqlashimiz mumkin: kiberxavfsizlik va tarmoq xavfsizligi.

Kiberxavfsizlik va tarmoq xavfsizligini tanganing ikki tomoni deb hisoblash mumkin. Ular, asosan, xodimlarning faoliyati va tarmoqqa kirishni tekshirish orqali ichki ma’lumotlarni himoya qilish uchun tarmoq xavfsizligini amalga oshirish uslubi bilan farq qiladi. Aksincha, kiberxavfsizlik tarmoqni buzib kirishgauringan xakerlar tomonidan yaratilgan xavfsizlik buzilishi kabi tashqi tahdidlarga qaratilgan.

Axborot, kiber va tarmoq xavfsizligini ta’minlash uchun kirish, maxfiylik, autentifikatsiya, yaxlitlik va rad etolmaslik kabi xususiyatlardan foydalaniladi.

Taqqoslash uchunasos	**Kiberxavfsizlik**	**Tarmoq xavfsizligi**
Asosiy	Qurilmalar va serverlarda joylashgan ma’lumotlarni himoya qilish mexanizmi.	Tarmoq orqali oqayotgan ma’lumotlarni himoya qilish uchun qulaylik sifatida xizmat qiladi.
Ichki qism	Axborot xavfsizligi	Kiberxavfsizlik
Hujum turlariga quyidagilar kiradi	Fishing, bahona, o‘lja.	Viruslar, troyan dasturlari, DOS hujumlari, xakerlik hujumlari va boshqalar.
O‘z ichiga oladi	Tarmoq himoyasi, dasturlar, dolzarb ma’lumotlar.	Hisob ma’lumotlari, Internetga kirish, xavfsizlik devorlari, shifrlash.

Kiberxavfsizlik nimani anglatishini tushunishdan oldin unga qanday tahdidlar va zaifliklar kiradi, biz kiber makon nima ekanligini tushunib olishimiz kerak. Kiber maydonda barcha turdagi aloqa tarmoqlari, ma’lumotlar bazalari, o‘rnatilgan protsessorlar, internet va elektron hujjatlarni almashtirish uchun tekshirgichlar birikmasi tasvirlangan. Butun dunyo bo‘ylab tarmoq muhiti telefon simlari, koaksiyal kabellar, elektromagnit to‘lqinlar va optik tolali liniyalar orqali hosil bo‘ladi. Kiber kosmik va internet atamalari bir-birining o‘rnida ishlatilishi mumkin bo‘lsa-da, bu kiber-makonning bir qismidir. Oddiy so‘zlar bilan aytganda, kiber kosmik - bu bog‘langan Internet muhiti.

Kiberxavfsizlik bu kiber makonni xurujlardan, noto‘g‘ri foydalanish, zarar yetkazish va iqtisodiy josuslikdan himoya qilish jarayonidir. Ba’zan olib tashlab bo‘lmaydigan o‘ziga xos zaifliklar kiber maydonga to‘sqinlik qilishi mumkin.

Tarmoq xavfsizligi - bu kiberxavfsizlikning bir qismi bo‘lib, bu yerda tarmoq bir nechta hostlarga va ularning xizmatlariga kirish shaxsiy host xavfsizligiga emas, balki e’tiborni boshqarishga qaratadi. Tarmoq xavfsizligi yechimlari uchta toifani o‘z ichiga oladi: apparat, dasturiy ta’minot va inson. Bu ma’lumotlar uzatish ustidan nazoratni qo‘lga kiritishga qaratilgan bo‘lib, bu tarmoq orqali qanday ma’lumotlar kelib tushishini va bizning tarmoqdan chiqib ketishni anglatadi. Tarmoqni himoya qilish va jismoniy kirishni boshqarish maqsadida amalga oshiriladigan boshqa funktsiyalar quyidagilardir: ma’lumotlarning tasodifiy buzilishidan saqlanish, ruxsatsiz tashqi bosqinlarni aniqlash va oldini olish hamda qasddan ichki xavfsizlik buzilishlarini oldini olish.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo‘lib, unga berilgan turlicha ta’riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta’rif berilgan: kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni to‘g‘ri bajarilishini kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o‘z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo‘lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o‘z ichiga oladi.

O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonunida unga quyidagicha ta’rif berilgan: “**Kiberxavfsizlik** — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati”.

Kiberxavfsizlikni fundamental atamalarini aniqlashga turli yondashuvlar mavjud. Xususan, CSEC2017 JTF manbasida mualliflar kiberxavfsizlikni quyidagi atamalari keltirishgan:

Konfidensiallik – axborot yoki uni eltuvchining shunday holati bo‘lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi. Konfidensiallik axborotni ruxsatsiz “o‘qish”dan himoyalash bilan shug‘ullanadi. AOB ssenariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob o‘z balansida qancha pul borligini Tridi bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma’lumotlarning konfidensialligini ta’minlash muhim hisoblanadi.

Yaxlitlik - axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati. Yaxlitlik axborotni ruxsatsiz “yozish”dan (ya’ni, axborotni o‘zgartirishdan) himoyalash yoki kamida o‘zgartirilganligini aniqlash bilan shug‘ullanadi. AOB ssenariysida Alisaning banki qayd yozuvi butunligini Tridi dan himoyalashi shart. Masalan, Bob akkauntida balansning o‘zgarishi yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

Bugungi kunda buzg‘unchilik, ma’lumotlarning buzilishi va kiberhujumlar har qachongidan ham tez-tez uchrab turadi. Aslida, shaxsiy yozuvlarni fosh qilgan ma’lumotlar buzilishi soni faqat 2015 va 2017 yillar orasida ikki baravar ko‘paydi . Ushbu hujumlarning ortib borayotgan soni va jiddiyligi tarmoq xavfsizligini, ayniqsa, hozirgi va istiqbolli sertifikatlangan IT mutaxassislari uchun eng muhim mavzuga aylantiradi .

CompTIA kiberxavfsizlik bo‘yicha keng qamrovli tadqiqotlar o‘tkazdi va xavfsizlik guruhlarini yaratish bo‘yicha yaqinda olib borilgan tadqiqotlar shuni ko‘rsatadiki, yangi xavfsizlik yondashuvining asosiy omili IT operatsiyalaridagi o‘zgarishdir. Bulutli provayderga o‘tish, yangi mobil qurilmalarni qo‘shish yoki ma’lumotlar tahliliga e’tibor qaratish - bularning barchasi yangi xavfsizlik taktikalarini talab qiladigan keng tarqalgan AT strategiyalari. Ushbu strategiyalar korporativ tarmoqdagi o‘zgarishlar yoki yaxshilanishlarga ham sabab bo‘lishi bejiz emas.Ushbu sohalarda muvaffaqiyatga erishish uchun tarmoq xavfsizligi bo‘yicha eng yaxshi amaliyotlarni chuqur tushunish kerak.

Tarmoq xavfsizligi kiberxavfsizlikning tarkibiga kiradigan kichikroq bo‘lim bo‘lib, u ruxsatsiz foydalanuvchilarning kompyuter tarmoqlari va ular bilan bog‘liq qurilmalarga kirishini oldini olish amaliyotini anglatadi.Bu tarmoq serverlari va qurilmalarini tashqi tahdidlardan jismoniy himoya qilishni, shuningdek, raqamli tarmoqni himoya qilish choralarini ko‘rishni o‘z ichiga oladi.Kiberhujumlar tobora murakkablashib borayotgan davrda tarmoq xavfsizligi har qachongidan ham muhimroq.

Tarmoq xavfsizligi ma’lumotlaringizning yaxlitligini hamda tashkilotingiz va xodimlaringiz maxfiyligini ta’minlash uchun juda muhimdir. U kuchli parollar yaratish va jamoat kompyuterlaridan to‘liq chiqish kabi eng oddiy amaliyotlardan tortib, tarmoqlar, qurilmalar va ularning foydalanuvchilarini xavfsiz saqlaydigan eng murakkab, yuqori darajadagi jarayonlargacha hamma narsani o‘z ichiga oladi. Ko‘proq va ko‘proq nozik ma’lumotlar onlayn va ushbu turli xil qurilmalarda saqlanadi va agar ruxsatsiz foydalanuvchi ushbu ma’lumotlarga kirish huquqiga ega bo‘lsa, bu halokatli natijalarga olib kelishi mumkin.

Tarmoq xavfsizligi ushbu maxfiy ma’lumotlarni xavfsiz saqlashning kalitidir va himoyasiz qurilmalarda ko‘proq shaxsiy ma’lumotlar saqlanganligi va baham ko‘rilgani sababli, tarmoq xavfsizligi faqat ahamiyat va zaruratni oshiradi. Mutaxassislar 2020 yilga kelib 2314 ekzabaytdan (yoki 2 trillion gigabaytdan ortiq) ma’lumotlar mavjudligini taxmin qilmoqdalar; bu miqdordagi ma’lumotlarni boshqarish etarlicha qiyin va uni himoya qilish butunlay boshqa masala bo‘ladi.

Tashkilotingizning har bir a’zosi narsalarni xavfsiz saqlashga yordam berish uchun qadam tashlashi mumkin bo‘lsa-da, so‘nggi yillarda tarmoq xavfsizligi yanada

murakkablashdi. Tarmoqlar va ularga ulangan qurilmalarni yetarli darajada himoya qilish tarmoqni keng qamrovli o‘qitishni, tarmoqlar qanday ishlashini to‘liq tushunishni va bu bilimlarni amalda qo‘llash ko‘nikmalarini talab qiladi. Maxfiylikni to‘liq saqlash uchun tarmoqlarni to‘liq va to‘g‘ri sozlash, himoyalash va nazorat qilish juda muhimdir.

Umumiy tarmoq xavfsizligi zaifliklari

Xavfsiz tarmoqlarni samarali tatbiq etish va qo‘llab-quvvatlash uchun bugungi kunda IT mutaxassislari duch keladigan umumiy zaifliklar, tahdidlar va muammolarni tushunish muhimdir. Ba’zilari juda oson tuzatilishi mumkin bo‘lsa-da, boshqalari ko‘proq jalb qilingan echimlarni talab qiladi.

Deyarli barcha kompyuter tarmoqlari tashqi hujumlarga ochiq qoladigan zaifliklarga ega; Bundan tashqari, hech kim ularga faol tahdid qilmasa yoki nishonga olmasa ham, qurilmalar va tarmoqlar hali ham himoyasiz. Zaiflik tashqi ta’sir natijasi emas, balki tarmoq yoki uning uskunasining holatidir.

Bular tarmoqning eng keng tarqalgan zaifliklari:

- Noto‘g‘ri o‘rnatilgan apparat yoki dasturiy ta’minot
- Yangilanmagan operatsion tizimlar yoki proshivka
- Noto‘g‘ri ishlatilgan apparat yoki dasturiy ta’minot
- Kambag‘al yoki jismoniy xavfsizlikning to‘liq etishmasligi
- Ishonchsiz parollar
- Qurilmaning operatsion tizimidagi yoki tarmoqdagi kamchiliklarni loyihalash

Zaiflik tajovuzkor yoki xaker sizning tarmog‘ingizni nishonga olishiga kafolat bermasa-da, bu ularga kirishni ancha osonlashtiradi va mumkin bo‘ladi.

Odamlar optik tizimlarni buzishning imkoni yo‘q deb o‘ylashadi . Biroq , IDC tadqiqot tahlilchisi Romain Fusherning ta’kidlashicha, optik tolali kabel tarmog‘ining mis kabellardan ko‘ra xavfsizroq ekanligi o‘zini oqlamaydi va yangi va arzon texnologiyalar endi ma’lumotlar o‘g‘irlanishini xakerlar uchun aniqlanmasdan osonlik bilan amalga oshirishga imkon berdi. Hisobotda qo‘shimcha qilinishicha, nozik ma’lumotlarni optik tolali kabellar orqali uzatuvchi tashkilotlar jinoiy tahdidlarga qarshi potentsial zaifdir, chunki kabelning ko‘p qismiga osongina kirish mumkin va etarli darajada himoyalanmagan.

Hakerlar ko‘pincha ilg‘or texnik nou-xauga ega bo‘lgan juda aqlli shaxslar sifatida tasvirlanadi. Ko‘pgina kiberjinoyatchilar ushbu tavsifga mos keladi, ammo tolali tarmoqni buzish uchun zarur bo‘lgan ko‘nikmalar bunday murakkablikni talab qilmaydi.

Fusherning aytishicha, optik tarmoqlarni buzishga shunchaki ultra yupqa tolalardan yorug‘lik olish orqali erishish mumkin. Muvaffaqiyatli teginishga

erishilgandan so‘ng, ma’lumotlarni yozib oladigan, kuzatadigan va tahlil qiladigan dasturiy ta’minot ma’lumotlarni yozib olishi mumkin. Hisobot moliyaviy, sug‘urta, sog‘liqni saqlash va davlat sektorlaridagi tashkilotlarni butun dunyo bo‘ylab optik tolali kabellar orqali nozik ma’lumotlarni yetkazib berishda juda ehtiyot bo‘lishlari haqida ogohlantiradi.

1990-yillardan boshlab optik tizimlarda kiberjinoyatchilik amaliyotning ko‘plab misollari mavjud:

- Fransiya va Shimoliy Koreya kabi davlatlar tarmoqni sanoat josusligi maqsadida buzib kirishgan.
- Al-Qoida AQSh va elchixonalar o‘rtasidagi suhbatlarni tinglagan
- 2000 yilda Deutsche Telekomning uchta asosiy magistral liniyasi buzilgan
- 2003 yilda Verizon optik tarmog‘iga maxfiy moliyaviy ma’lumotlarga kirish uchun foydalanilgan deb hisoblangan qurilma orqali kirilgan.

XULOSA VA MUNOZARA

Optik tarmoqlar xizmatni buzish yoki tizimga ruxsatsiz kirishni maqsad qilgan bir necha turdagi xavfsizlik buzilishlariga nisbatan zaifdir. Dasturlashtiriladigan va moslashuvchan tugun arxitekturasi dasturiy ta’minotining evolyutsiyasi tarmoqni loyihalash va ishlatish jarayonida hisobga olinishi kerak bo‘lgan yangi xavfsizlik zaifliklariga olib keldi. Ushbu bo‘lim joriy va kelajakdagi optik tarmoqlardagi potentsial xavfsizlik muammolari haqida umumiy ma’lumot beradi va tegishli zaifliklardan foydalanadigan mumkin bo‘lgan hujumlarni aniqlaydi. U identifikatsiya, autentifikatsiya, yaxlitlik, xizmat ko‘rsatishni rad etish va maxfiylikni o‘z ichiga oladi. Buzg‘unchi optik tolaga tegib yoki qo‘shni maxfiy signallar spektridan tarqaladigan interferentsiya orqali yashirinishi mumkin va ancha vaqt davomida aniqlanmaydi.

ADABIYOTLAR RO‘YXATI

1. S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: o’quv qo’llanma. – T.: «Aloqachi», 2020, 208 bet.
2. White. Gregory B. “Computer system and network security” CRC Press-1996
3. Ben Wu, Bhavin Shastri, Paul Prucnal. “Secure Communication in Fiber-Optic Networks” , Emerging Trends in ICT Security, Pages 162-189, 2014.
4. Khillar, Sagar. "Difference between Cyber Security and Network Security." Difference Between Similar Terms and Objects, 17 July, 2018
5. Singh, Kunal, "Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab" (2020). Master’s Theses (2009 -). 402.