****

**O`ZBEKISTON RESPUBLIKASI OLIY VA O`RTA MAXSUS**

**TA`LIM VAZIRLIGI**

**MIRZO ULUG`BEK NOMIDAGI O`ZBEKISTON MILLIY UNIVERSITETI**

**JIZZAX FILIALI**

**“AMALIY MATEMATIKA” FAKULTETI**

**“Amaliy matematika va informatika” KAFEDRASI**

**“Axborot xavfsizligi’’ yo’nalishi**

**30-21-guruh**

**“Axborotni himoyalashning texnik usullari va vositalari” FANIDAN**

***5-Amaliy mashg‘ulot***

**Bajardi: Quvondiqov H**

**Qabul qildi: Baratov J**

**Jizzax 2024**

**Mavzu: Soxta elektromagnit emissiya va shovqinlarning (PEMIN)**

PEMIN (soxta elektromagnit nurlanish va interferensiya) atamasi 60-yillarning oxiri va 70-yillarning boshlarida elektron jihozlardan har xil turdagi niqobni ochish va adashgan emissiyalar orqali maʼlumotlar sizib chiqishini oldini olish usullarini ishlab chiqishda paydo boʻlgan. Evropa va Kanadada bu atama ishlatiladi "kompromatli emanatsiya" - kompromat nurlanish. PEMINning namoyon bo'lishi 18-asrda kuzatilganiga qaramay, to'liq miqyosli tadqiqotlar Ikkinchi Jahon urushi davrida boshlandi, bu birinchi bo'lib chiqdi. O‘z navbatida , ishtirokchi mamlakatlar hukumatlarining o'z ma'lumotlarini sir saqlash va olish istagi dushman ma'lumotlariga kirish *.*Axborot xavfsizligi nuqtai nazaridan PEMIN xavfi birinchi marta 1985 yilda "Video displey modullaridan elektromagnit nurlanish” maqolasini nashr etgan golland muhandisi Vim van Ek tomonidan aniq ko'rsatildi. Maqola video monitorlarning kompozit signalini ushlab turishning potentsial usullariga bag'ishlangan. 1985 yil mart oyida Kannda bo'lib o'tgan Securecom-85 ko'rgazmasida van Ekk monitor emissiyasini ushlab turish uchun uskunalarni namoyish etdi. Tajriba juda oddiy edi: ko'chada to'xtab turgan mashinada antennasi yaxshilangan oddiy televizor qabul qiluvchisi o'rnatildi, uning ekranida xuddi shu tasvirni ko'rish mumkin edi.mashina yonidagi binoda kompyuter monitori *.*Tajriba shuni isbotladiki, ma'lumotni monitordan ushlab olish biroz o'zgartirilgan an'anaviy televizor qabul qilgich yordamida mumkin. PEMIN manbalari bo'lgan jarayonlar va hodisalarni to'rt turga bo'lish mumkin:

1. tashqi akustik signallarni radiotexnika va elektr qurilmalarning funktsiyalarida ko'zda tutilmagan elektr signallariga aylantirish;

2. past chastotali soxta emissiyalar;

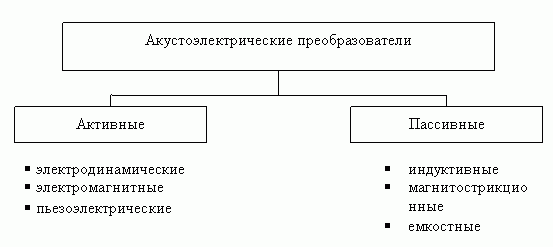
3. soxta yuqori chastotali emissiyalar;

4. parazitar aloqalar va interferensiya.

Keling, ushbu PEMIN turlarining har birini batafsil ko'rib chiqaylik.

**Akustik signallarni elektr signallariga yon konvertatsiya qilish**

Akustoelektrik o'zgartirgichlar tashqi akustik signallarni elektrga aylantiruvchi deb ataladi. Akustoelektrik transduserlar turli xil elementlar, qismlar va moslamalarni o'z ichiga oladi akustik to'lqin ekvivalent elektr signallarini yaratadi yoki ularning parametrlarini o'zgartiradi.



Har qanday kompyuterning ishlashi paytida yuzaga keladigan atrof-muhit elektromagnit nurlanishi va shovqinlari (PEMIN) tarmoqqa ulanmagan uskunadan ma'lumotni olib tashlash usulidir. Tahdid darajasini amaliy nuqtai nazardan baholash kerak, professional elektron xavfsizlik moslamalarini o'rnatish xarajatlar va ofisga kirish bilan bog'liq. Bunday choralar faqat juda qimmatli ma'lumotlarni olish uchun amalga oshiriladi.

**PEMIN kanallari qanday ishlaydi**

Elektromagnit kuchlanish kompyuter arxitekturasining har qanday elementining ishlashi paytida yuzaga keladi. Ba'zi hollarda u axborot signali bilan modulyatsiya qilinadi. Radiatsiyani ushlab turish va shifrni ochish tajovuzkorning ma'lumot olishiga olib keladi. Qabul qiluvchi elektron qurilmalar kompyuterga o'rnatiladi, quvvat yoki topraklama tarmoqlariga parallel ravishda ulanadi, oddiygina ishlaydigan uskunaga yaqin joylashtiriladi yoki antenna yordamida ma'lumotlarni ushlab turadi.

PEMIN kanallari orqali ma'lumotlarning chiqib ketishi sodir bo'ladi:

elektromagnit kanallar orqali. Radiatsiya R2 zonasida tarqaladi, FSTEC standartlari bo'yicha himoyalangan uskunalar uchun uning radiusi 8-10 m dan oshmaydi.Himoyalanmagan trubkali televizor tipidagi monitor nurlanishni tarqatadi, uni qabul qiluvchi qurilmada axborot signaliga aylantirish mumkin. 100 m gacha bo'lgan masofada joylashgan;

elektr kanallari orqali. Signal quvvat va tuproq simlari orqali o'tadi. Ulardan shovqin boshqa tarmoqlarning simlariga uzatiladi va himoyalangan hududdan tashqarida tutilishi mumkin.

Ko'pincha radiatsiya quyidagilar tomonidan ishlab chiqariladi:

1. monitorda ma'lumotlarni ko'rsatishda;

2. klaviaturadan ma'lumotlarni kiritishda;

3. ma'lumotlarni qattiq diskka yozishda yoki olinadigan muhitdan nusxalashda.

Elektron ma'lumotlarni ushlash qurilmalari signalni tashqi tomondan qabul qiluvchi qurilmaga uzatadi, odatda ma'lumotni radio signaliga aylantiradi. Uzatuvchining chastotasi yoki chastota spektriga sozlangan tajovuzkorning radio qabul qilgichi bino yaqinida, to'xtab turgan mashinada yoki kuchli uzatuvchi ishlatilsa, 10 km gacha bo'lgan masofada joylashgan bo'lishi mumkin.

**Hujum va tahdidlar**

PEMIN kanallari orqali ma'lumotlarning chiqib ketishining potentsial xavfini hisobga olgan holda tahdid modeli himoyalangan ma'lumotlarning haqiqiy qiymatiga asoslanishi kerak. Rossiya Federatsiyasi FSTEC ularni uch guruhga ajratadi:

birinchi sinf. Axborotning qiymati uning egasi tomonidan mustaqil ravishda belgilanadi;

ikkinchi sinf. Axborot tizimi qonun bilan cheklangan kirish huquqiga ega bo'lgan ma'lumotlarni (bank siri, tibbiy maxfiylik) yoki shaxsiy ma'lumotlarni qayta ishlaydi;

uchinchi sinf. Tashkilot davlat sirlarini tashkil etuvchi ma'lumotlar bilan ishlaydi.

Agentlik hujumchilarni guruhlarga ajratadi - past, o'rta va yuqori salohiyatli. PEMIN kanallari orqali sizib chiqish tahdidlarini amalga oshirish uchun ikkinchi va uchinchi guruhlar darajasidagi tajovuzkorlarning uskunalari va ko'nikmalari talab qilinadi - biznes josusligi yoki xorijiy texnik razvedka sohasidagi mutaxassislar.

Shunga ko'ra, ushbu toifadagi agentlarni qiziqtiradigan qimmatli ma'lumotlar bilan ishlaydigan tashkilotlar PEMIN kanallari orqali sizib chiqishi haqida tashvishlanishlari kerak. Yuqori darajada, mutaxassislar mavjud shovqinlarni oddiygina olib tashlash bilan cheklanmaydi. Ular zararli dasturlarni kompyuterga kiritishga qodir, ular kerakli ma'lumotlarni topadilar va uni ushlab qolish uchun qo'shimcha signallarni yaratadilar.

**Elektromagnit radiatsiyani to'xtatish**: Faraday bo'yida kafolatlangan xona, ichiga kira elektromagnit radiatsiyani jamlab, tarmoq ichidagi qurilmalarga yetib borishini oldini oladi. Metal kafolatlangan xona, elektromagnit dastgohlarni tashqi tajovuzlardan himoyalaydi, shuningdek, ularning o'zining tizimlari orqali yaratilgan radiatsiyani qayta ishlashni cheklashga yordam beradi.

**Elektr radiatsiyani to'xtatish:** Bunday xonalar elektr radiatsiyani ham to'xtatish uchun samarali bo'ladi. Faraday bo'yida kafolatlangan xona, elektr tajovuzlarni kamaytirish va unga qarshi qarshiya ko'rsatish uchun ideal bo'lib, shuningdek, o'zining tizimlari orqali elektr radiatsiyasini ham kamaytiradi.

**Radiatsiya yo'qotish:** Faraday bo'yida kafolatlangan xona, ichiga kira radiatsiyani yig'ishni ta'minlaydi, shuningdek, uni chiqarishga imkon beradi. Bu xona, ma'lumotlar tarmoqlarini tashqari radiatsiyalardan himoyalash, shu jumladan, radiofrekans radiatsiyasi, xususan, elektronik qurilmalar uchun juda muhimdir.

**Davlatlararo xavfsizlik tajribalari va laboratoriyalarda ishlatilishi:** Faraday bo'yida kafolatlangan xonalarning muhim foydalanilishlari laboratoriyalarda, davlatlararo xavfsizlik tajribalari va soddalashlar jihatidan amalga oshiriladi. Ular, radiatsiya yolg'onlarini o'rganish, shuningdek, elektronik qurilmalarni radiatsiya tajovuzlariga qarshi sinash va xavfsizligini ta'minlashda foydalaniladi.

Faraday bo'yida kafolatlangan xonalarning belgilangan xususiyatlari quyidagicha:

**Materiallar**: Faraday bo'yida kafolatlangan xonalarda metallar ishlatiladi, masalan, temir, medi, yoki alumin.

**O'lcham:** Xonalarning o'lchami qanchalik katta bo'lsa, ular shuncha kuchliroq bo'ladi. Ammo, hajmi ham muhimdir - kafolatlangan xonaning ichki hajmi, tarmoq qurilmalarini va ularning vositalarini o'z ichiga olishi kerak

**Shakli**: Faraday bo'yida kafolatlangan xonalar, har xil shakllarda ishlab chiqarilishi mumkin - qutbiy, kublik, yoki silindrik shakl. Shakl, xonaning qaysi maqsadlarga mos kelishiga bog'liq bo'ladi.

**Himoya darajasi:** Xonalarning himoya darajasi, ularni elektr va elektromagnit radiatsiyadan qanchalik himoyalashini aks ettiradi. Yuqori himoya darajali xonalar, yuqori kuchli radiatsiyani to'xtatishga qodir bo'ladi.

***PEMIN filtrlarining vazifalari va harakteristikalari quyidagi:***

**Radiatsiyani qisqartirish:** PEMIN filtrlari, elektronik ma'lumotlarni ta'minotini yuqori darajada ta'minlash uchun ishlab chiqarilgan tizimlardir. Ular, ma'lumotlar tarmoqlariga kiruvchi elektr va elektromagnit radiatsiyani kamaytirish uchun mo'ljallangan.

**Tizimning tajovuzga qarshi muhofazasi:** PEMIN filtrlari, tarmoq tizimlarini tajovuzlarga qarshi himoya qilishda kritik ahamiyatga ega. Ular, tarmoqda yutuq radiatsiyani cheklash, tarmoq tizimini tajovuzlardan himoyalash, shuningdek, tarmoq xavfsizligini ta'minlash uchun foydalaniladi.

**Elektronik qurilmalarni himoyalash:** Filtrlar, elektronik qurilmalarga kiruvchi yutuq radiatsiyasini kamaytirish uchun mo'ljallangan. Bu, qurilmalar uchun zararli bo'lgan radiatsiyani qisqartirish va ularning ishlashini ta'minlashda muhim rol o'ynaydi.

**Xavfsizlikni ta'minlash:** PEMIN filtrlari, tarmoq tizimlarini tajovuzlarga qarshi himoya qilishda muhim vazifalarni bajaradi va bu, elektronik tarmoqlarning xavfsizligini ta'minlashda yordam beradi. Ular, hujjatlar va ma'lumotlarni himoya qilish uchun muhimdir.

PEMIN filtrlarining quyidagi harakteristikalari mavjud:

**Chastotasi:** Filtrlarning ishlash spektri, ularga kiruvchi radiatsiya turlariga bog'liq bo'ladi. Ba'zi filtrlar shunchaki radiofrekans spektrumida ishlaydi, shuningdek, boshqalar xil turlardagi elektr va elektromagnit radiatsiyasini ham qisqartirish uchun mo'ljallangan.

**O'lcham va shakli:** Filtrlar, tarmoq tizimining o'lchami va shakli bilan mos kelishi kerak. Ularning o'lchami va shakli, ularni ma'lumotlar tarmoqlariga moslashtirish va ularga o'rnatishda ishlatiladi.

**Ishtirok etadigan qurilmalar soni:** Filtrlarning tizimda qancha qurilmalar bilan ishlay olishi kerakligi ham muhimdir. Ishlatilgan qurilmalar soni, tizimning ta'minoti va xavfsizligi uchun kritik bo'ladi.

**Xususiy ravishda yoritilgan himoya darajasi:** PEMIN filtrlari, tarmoq tizimlarini himoyalashda muhim bo'lgan kuchli himoya darajasiga ega bo'lishi kerak. Ularning himoya darajasi, tarmoq tizimi tajovuzlariga qarshi himoyalashda kritik ahamiyatga ega.

***Elektromagnit va shovqin sensorlari*** elektronik tarmoqlarda yuzaga keladigan elektromagnit va shovqin radiatsiyasini aniqlash va nazorat qilish uchun mo'ljallangan vositalardir. Ular, tarmoq xavfsizligini ta'minlash, radiatsiyani o'rganish va uni tushirish, shuningdek, ma'lumotlarni himoya qilishda juda muhim rol o'ynaydilar.

**Radiatsiya aniqlash**: Elektromagnit va shovqin sensorlari, tarmoq tizimlarida yuzaga keladigan elektr va elektromagnit radiatsiyasini aniqlaydi. Ular, radiatsiya darajasini nazorat qilish, uning o'zgarmasini aniqlash va radiatsiya darajasini aniqlangan limitlar ichida saqlashda yordam beradi.

**Tajovuzlarni aniqlash va xavfsizlikni ta'minlash**: Sensorlar, tarmoq tizimlariga tajovuz qilishga harakat qilayotgan yoki tajovuz qilingan qurilmalarni aniqlashda ham ishlatiladi. Ular, yomoniyatni aniqlash, tizimni radiatsiya tajovuzlariga qarshi himoya qilish va xavfsizligini ta'minlashda yordam beradi.

**Ovoz va elektromagnit sensorlari:** Ba'zi sensorlar ovoz radiatsiyasini ham o'rganishi mumkin. Bu sensorlar, tarmoq tizimlarida yuzaga keladigan elektromagnit va ovozli radiatsiyani birgalikda nazorat qilishda ishlatiladi

**Tajovuzlarni tugatish va ogohlantirish:** Sensorlar, tajovuz qilingan paytda tizimni ogohlantirish, tajovuzlarni aniqlash va uni tugatishda yordam beradi. Misol uchun, agar tajovuz qilingan paytda sensor radiatsiya darajasining limitlarini oshib ketganini aniqlasa, tarmoq tizimiga ogohlantirish berishi mumkin.

*Elektromagnit va shovqin sensorlarining quyidagi harakteristikasi mavjud:*

**Chastotasi:** Sensorlar, aniqlaydigan radiatsiya turlari, masalan, radiofrekans, infrachervona, ovoz, va boshqalari bo'yicha farqli bo'lishi mumkin. Har bir sensorning ishlash chastotasi va yo'nalishi mavjud bo'ladi.

**Chuqurlik va dastlabki ta'minot qobiliyati:** Sensorlar, ma'lumotlarni chuqurlik darajasi va tarmoq tizimining o'lchami bilan moslashishi kerak. Ularning ogohlantirish qobiliyati va tugatishdarajalari tizimning xavfsizligi va himoyalashida kritik ahamiyatga ega bo'ladi.

**Energiya sarflanishi**: Sensorlar o'zlariga energiya ta'minotini zarur qiladi. Shuningdek, ularning energetik xavfsizligi ham juda muhimdir, chunki ular tarmoq tizimining ishga tushishida yordam beradi.

**O'zgaruvchanlik va dinamikasi**: Ba'zi sensorlar o'zgaruvchan va dinamik bo'lishi kerak, shuningdek, radiatsiya darajalarining o'zgarishlariga tez va to'g'ri javob berishi kerak. Bu, tarmoq xavfsizligini saqlashda va tajovuzlarni aniqlashda juda muhimdir.

***Radiatsiya qayta ishlovchi qurilmalar (Radiation Hardened Devices)*** elektronik qurilmalarni yoritilgan yoki yoritilmagan radiatsiya sharoitlarida ishlash uchun mo'ljallangan qurilmalardir. Bu qurilmalar, kosmik tarmoq, noyob radiatsiya muhitlari, yoki yoritilmagan industrial muhitlar kabi yoritilmagan radiatsiya sharoitlarida ishlab chiqarilgan elektronik qurilmalarga moslashtirilgan.

**Radiatsiya to'xtatish**: Radiatsiya qayta ishlovchi qurilmalar, yoritilgan yoki yoritilmagan radiatsiya muhitlari ichida elektronik qurilmalarni himoya qilish uchun ishlatiladi. Ular, elektronik qurilmalarning ishlashini radiatsiyani to'xtatib, ularga zarar yetkazmaslik uchun mo'ljallangan.

**Radiatsiya darajasini nazorat qilish**: Bu qurilmalar radiatsiya darajasini monitoring qilish va elektronik qurilmalar uchun zararli darajadagi radiatsiyani aniqlashda yordam beradi. Shuningdek, ulardan olinayotgan ma'lumotlar tizimlarga radiatsiya tajovuzlarini aniqlashda yordam beradi.

**Radiatsiya ga'zib qilish**: Radiatsiya qayta ishlovchi qurilmalar, radiatsiyani ga'zib qilish va qarshilik qilishda ishlatiladi. Ularning ichida qo'shimcha himoyalash qurilmalari mavjud bo'lib, radiatsiya tajovuzlarini pastga tushirish uchun qo'shimcha himoya ta'minlaydi.

**O'zgarishsiz ishlovchi:** Bu qurilmalar, yoritilgan yoki yoritilmagan radiatsiya sharoitlarida dastlabki ishlovchi sifatida ishlovchi vaqtida xato qilishsiz ishlovchi bo'lishi uchun mo'ljallangan.

**Xavfsizlikni ta'minlash:** Radiatsiya qayta ishlovchi qurilmalar, tarmoq tizimlari va qurilmalarni yoritilgan radiatsiya sharoitlarida ishlashga tayyorlashda yordam beradi. Ularning qo'shimcha himoya funksiyalari, tarmoq tizimlarini radiatsiya tajovuzlari va tajovuzlarni qayta ishlovchi qurilmalardan himoyalashda muhimdir.

Radiatsiya qayta ishlovchi qurilmalar, elektronik qurilmalarni yoritilgan yoki yoritilmagan radiatsiya muhitlari ichida ishlash uchun mo'ljallangan. Ularning vazifalari tarmoq xavfsizligini ta'minlash, radiatsiya tajovuzlarini pastga tushirish va elektronik qurilmalarni himoya qilishga yo'naltirilgan.

***Tarmoq xavfsizligi monitorlash va nazorat qilish tizimlari***: Bu maxsus tizimlar, tarmoq tizimlarini radiatsiya tajovuzlari va tajovuzlarni qayta ishlovchi qurilmalar to'g'risida nazorat qilishda ishlatiladi. Ularning yordamida, tarmoq xavfsizligi mutaxassislarining radiatsiya darajasini nazorat qilishi va tajovuzlarni aniqlashi mumkin.

Tarmoq xavfsizligi monitorlash va nazorat qilish tizimlari, elektronik tarmoq tizimlarining xavfsizligini nazorat qilish va himoya qilish uchun mo'ljallangan maxsus qurilmalar va dasturlar to'plamidir. Bu tizimlar, tarmoq tizimlarida yuzaga keladigan tajovuzlarni aniqlash, ularga qarshi himoya tizimlarini faollashtirish, va xavfsizlik holatini nazorat qilishda yordam beradi.

Quyidagi misollar tarmoq xavfsizligi monitorlash va nazorat qilish tizimlari uchun bo'lishi mumkin:

**SIEM (Security Information and Event Management) tizimlari:** SIEM tizimlari, tarmoq tizimlaridan kelgan ma'lumotlarni to'plab, tahlil qilish, va tarmoq xavfsizligi uchun tahlil qilishda ishlatiladi. Ularning ichida harakat kuzatuvchi, tarmoq qavatlarini kuzatuvchi, va tarmoq tizimlarining holatini nazorat qilish imkoniyatlari mavjud.

**IDS (Intrusion Detection Systems) va IPS (Intrusion Prevention Systems):** IDS va IPS tizimlari, tarmoqda yuzaga keladigan tajovuzlarni aniqlash va ularga qarshi harakat qilishda ishlatiladi. IDS tizimlari tarmoqdagi zararli harakatlarni aniqlab chiqaradi, unga reagiratsiya qiladi, va haqiqiy vaqtida ogohlantirish beradi. IPS tizimlari esa tajovuzlarni to'xtatish, bloklash yoki izchil qilish uchun faollashtiriladi.

**Firewall tizimlari:** Firewall tizimlari, tarmoqni tajovuzlardan himoyalash uchun asosiy qo'llanma hisoblanadi. Ular, tarmoq qavatlarini va tarmoq qurilmalarini himoya qilish uchun xavfsizlik siyosatlarini qo'llaydilar, tarmoq trafikini kuzatish va zararli trafikni bloklaydilar.

Antivirus va antimalware dasturlari: Bu dasturlar, kompyuterlarga o'rnatilgan viruslar va zararli dasturlarni aniqlash va unga qarshi harakat qilishda yordam beradi. Ular, kompyuterlarni himoya qilish va radiatsiya tajovuzlarini pastga tushirishda muhim rollarni o'ynaydilar.

**Network Access Control (NAC) tizimlari:** NAC tizimlari, tarmoqga kirishni nazorat qilish uchun ishlatiladi va tarmoqqa kirish uchun to'g'ri huquqni ta'minlashda yordam beradi. Ularning ichida foydalanuvchilar, qurilmalar, va tarmoq qurilmalari uchun kirish shartlari va huquqlarini boshqarish imkoniyatlari mavjud. Bu misollar tarmoq xavfsizligi monitorlash va nazorat qilish tizimlari uchun misol bo'lishi mumkin. Ularning yordamida tarmoq xavfsizligi nazorat qilish, zararli tajovuzlarni aniqlash va ularga qarshi harakat qilish, tarmoq trafikini kuzatish va himoya qilish imkoniyatlariga ega bo'lish mumkin.