O`ZBEKISTON RESPUBLIKASI ALOQA, AXBOROTLASHTIRISH VA TELEKOMMUNIKATSIYA TEXNOLOGIYALARI DAVLAT QO`MITASI

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI NUKUS FILIALI

KOMPYUTER INJINIRINGI FAKULTETI

«TELEKOMMUNIKATSIYA INJINIRINGI» KAFEDRASI

Mavzu: «*Ma`lumotlar uzatish tarmoqlarida xavfsizlik taxdidlarini taxlili* » mavzusidagi

BITIRUV MALAKAVIY ISHI

Bajardi: «5522200-telekommunikatsiya» ta`lim yo`nalishi bitiruvchi 4 kurs talabasi
Djumamuratova.N._____

ILMIY RAXBAR:
Radioteleuzatish markazi direktori
.Xalbaev.E_____

Bitiruv malakaviy ishi kafedradan dastlabki himoyadan o`tdi.
_____ sonli bayonnomasi «_____» _____ 2014 yil

Nukus – 2014y

O`ZBEKISTON RESPUBLIKASI ALOQA, AXBOROTLASHTIRISH VA TELEKOMMUNIKATSIYA TEXNOLOGIYALARI DAVLAT QO`MITASI

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
NUKUS FILIALI

“Komp`yuter injiniringi”fakul`teti

“Telekommunikatsiyainjiniringi”
kafedrasi

5522200 – Telekommunikatsiya bakalavr ta`lim yo`nalishi

“Tasdiqlayman”
Telekommunikatsiya injiniringikafedrasimudiri
_____ K.O.Tleuov
«____» _____ 2014 y

Djumamuratova Nargiza Kamiljanovnaning

(Familiyasi ,Ismi, Otasining ismi)

Malakaviy ish mavzusi: ***“Ma`lumotlar uzatish tarmoqlarida xavfsizlik taxdidlarini taxlili”*** mavzuyidagi bitiruv ishiga oid

TOPSHIRIQ

1. TATU Nukus filialining № 122 buyrug`i bilan2014- yil **“** 4-mart**”** da tasdiqlangan.
2.Malakaviy ishni topshirish muddati: 2014 yil 5 - iyun`
3. Ishiga oid dastlabki ma’lumotlar *Diplom oldi amaliyoti va adabiyotlar*
4. Hisoblash tushintirish yozmalar mazmuni (ishlab chiqiladigan masalalarning ro’yxati).

1. *Ma`lumotlarni uzatish tarmog’ida axborotni ximoyalash.* ***2***. *Axborot xavfsizligiga taxdidlar.* ***3***. *Ma`lumotlar uzatish_tarmoqlarida xavfsizlik taxdidlarini taxlili.* ***4***. *Xayot faoliyati xavfsizligi*

5. Grafik materiallar ro`yhati *Prezentatsiya*

6. Topshiriq berilgan sana 26.01.2014

Rahbar _____
imzo

Topshiriq oldim _____
imzo

7. Ishning ayrim bo`limlari bo`yicha maslaxatchilar:

Bo`lim nomi	Maslahatchi	Imzo, sana	
		Topshiriqberildi	Topshiriq Olindi
. Asosiyqism	Xalbaev E	26.01.2014	

8. Ishni bajarish grafigi

T/r	Ish bo`limlari nomi	Bajarish muddati	Rahbar (maslahatchi) imzosi
1.	Ma`lumotlarni uzatish tarmog'ida axborotni ximoyalash.	21.02.2014	
2.	Axborot xavfsizligiga taxdidlar.	19.03.2014	
3.	Ma`lumotlar uzatish_tarmoqlarida xavfsizlik taxdidlarini taxlili.	20.04.2014	
4.	Xayot faoliyati xavfsizligi	26.05.2014	

Bitiruvchi_____ 2014yil «_____»_____
imzo

Rahbar_____ 2014yil «_____»_____
imzo

KIRISH

Ildam qadamlar bilan rivojlanayotgan Kompyuter axborot texnologiyalari xayotimizda sezilarli o’zgarishlarga sabab bo’lmoqda. "Axborot" tushunchasi sotib olish, sotish, biror narsaga almashish va x. mumkin bo’lgan maxsus tovarni belgilashda tez-tez ishlatila boshlandi. Bunda axborotning narxi ko’pincha u joylashgan Kompyuter tizimi narxidan yuz va ming marta yuqori bo’ladi. Demak, axborotni ruxsatsiz foydalanishdan, atayin o’zgartirishdan, yo’q qilishdan va boshqa jinoiy xarakatlardan ximoyalash zaruriyatining paydo bo’lishi tabiiydir.

Axborotni ximoyalash muammosi Kompyuter tizimlari va tarmoqlari soxasida faoliyat ko’rsatuvchi mutaxassislar xamda zamonaviy Kompyuter vositalaridan foydalanuvchilar e`tiborini jalb etmoqda.

Axborot xavfsizligini ta`minlash muammosi Internetning ishlash sharoitlarida muhim ahamiyat kasb etadi. Mutloq ko’pchilik kompaniya va tashkilotlar bugungi kunda o’zlarining lokal tarmoqlarini Internetga, uning resurslari va afzalliklaridan foydalanish uchun ulamoqdalar. Ular Internetni turli maqsadlarda ishlatadilar, bunga elektron pochta bilan almashinish, qiziqib qolgan shaxs va tashkilotlar o’rtasida axborotlarni olish va tarqatish va boshqalar kiradi. Bosh tarmoqqa ulanish katta afzallikga ega, ammo bunda ulanayotgan lokal yoki korporativ tarmoqdagi axborot xavfsizligini ta`minlashda jiddiy muammolar paydo bo’ladi. O’zining idealogiyasidagi ochiqchilik tufayli Internet yomon niyatli odamlarga, muhim va maxfiy axborotni o’g’irlash, xalaqitlarga uchratish va buzish maqsadida korxona va tashkilotlarning ichki tarmoqlariga kirish uchun ko’p imkoniyat yaratib beradi. Axborot juda axamiyatli yoki o’ta muhim bo’lganligi sababli bunday axborotni saqlayotgan, qayta ishlayotgan yoki uzatayotgan Kompyuter tizimlari va tarmoqlariga nisbatan turli xil yomon niyatli xarakatlar bo’lishi mumkin.

Internetni tadbiq qilinishi bilan jinoyatlar ayniqsa keng quloch yoydi. Bu esa qonuniyatlidir, negaki ShK ning faol ishlatilishining birinchi o’n yilligida Kompyuterlarga asosan telefon tarmog’i orqali ulanib olgan xakerlar yoki

«elektron qaroqchilar» asosiy xavf-xatarga ega bo’lgan bo’lsa, unda Kompyuter tizimlarini va tarmoqlarini ommaviy ishlatish davrida axborotning ishonchliligi va butunligini buzishga Kompyuter viruslari dasturlari va Internet global tarmoqi orqali xavf solinmoqda.

«Axborotni qanday ximoya qilish kerak?» savoli bilan himoya qilish tizimi tushunchasi, ya`ni tadbir va vositalar kompleksi hamda ular asosida himoya qilish ob`ektining xavfsizligi xavflarini turli – tuman ko’rinishlarini payqash, qaytarish va yo’q qilishga yo’naltirilgan faoliyat ajralmas ravishda bog’langandir.

Axborotni ximoyalashda tarmoqlararo ekranlarning funktsiyalari taxlil etilib, ularning OSI modelining turli satxlarida ishlashi xususiyatlari muxokama qilinadi. Tarmoqlaro ekranlar asosida tarmoqni ximoyalash sxemalari tavsiflanadi.

1. MA`LUMOTLARNI UZATISh TARMOG'IDA AXBOROTNI XIMOYaLASh

1.1. Ma`lumotlarni uzatish tarmoqlarida axborot ximoyasini ta`minlash

Ma`lumotlarni uzatish tarmoqlarida axborot ximoyasini ta`minlash masalasi ma`lumotlar uzatish tarmog'ining muayyan arxitekturasini amalga oshiruvchi va uning barqaror ishlashini ta`minlovchi apparat-dasturiy vositalari bilan bog'liq xolda yechilishi lozim.

Ma`lumotlarni uzatish tarmoqlarida axborot xavfsizligini ta`minlashga quyidagi talablar quyiladi:

- ma`lumotlarni uzatish tarmoqlarida axborot xavfsizligiga bo'ladigan ma`lum taxdidlardan ximoyalash xizmati va mexanizmlarini belgilovchi *funktsional talablar*;

- axborot xavfsizligiga bo'ladigan ma`lum taxdidlardan ximoyalash mexanizmini ma`lumotlarni uzatish tarmog'i arxitekturasiga qay tarzda joriy etilishi lozimligini belgilovchi *arxitekturaviy talablar*;

- boshqarishning qanday funktsiyalari ishlab chiqilishi va ular qay tarzda ma`lumotlarni uzatish tarmog'iga joriy etilishini belgilovchi *boshqarish (ma`murlash) talablari*.

Funktsional talablar. Ma`lumotlarni uzatish tarmog'i komponentlariga va arxitekturasiga real ta`sir etuvchi umumiy funktsional talablar quyidagilar:

- *foydalanuvchini autentifikatsiyalash.* Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta`minlovchi tizim axborotni (ma`lumotlarni) uzatish jarayonida ishtirok etuvchi komponentining (ob`ekt, sub`ekt va foydalanuvchining) xaqiqiyligini aniqlash imkoniyatini ta`minlashi lozim;

- *nazoratlanuvchi foydalanish.* Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta`minlovchi tizim tarmoq sub`ektlari va foydalanuvchilarining ruxsat etilmagan axborot resurslaridan foydalana olmasliklarini kafolatlashi lozim;

- *konfidentsiallikni ta`minlash.* Konfidentsiallikni ta`minlash xizmati asosan ma`lumotlarni uzatish tarmog'ini axborot muxitini ochish, axborotdan ruxsatsiz foydalanish va o'g'irlash imkoniyatlaridan ximoyalash uchun zarur xisoblanadi;

- *ma`lumotlar yaxlitligini ta`minlash.* Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta`minlovchi tizim tarkibida foydalanuvchi va boshqarish axboroti bo'lgan ma`lumotlarning saqlanish va uzatilish yaxlitligini kafolatlashi lozim. Ma`lumotlarning buzilishi, soxtalashtirilishi, kechiktirilishi, ruxsatsiz qaytalanishi axborot uzatilishininig blokirovka qilinishiga olib kelishi mumkin;

- *qat`iy xisob-kitob*. Ma`lumotlarni uzatish tarmog'i resurslaridan foydalanuvchi xar qanday sub`ekt bajargan xar qanday amallari uchun javob berishi lozim. Ma`lumotlarni uzatish tarmog'i ustida qilingan barcha xarakatlar va tarmoqda sodir bo'lgan barcha xodisalar xususidagi axborotning saqlanish imkoniyati ta`minlanishi lozim;

- *xavfni bildiruvchi signalni generatsiyalash*. Ma`lumotlarni uzatish tarmog'i tarmoq axborot xavfsizligi ob`ektlari tomonidan xavfsizlikning buzilishi xususidagi signalni generatsiyalash imkonini ta`minlashi lozim;

- *audit.* Audit tizimni boshqarishning samaradorligini baxolash xamda axborot xavfsizligining buzilishini aniqlash maqsadida tizimli yozuvlarni va amallarni mustaqil taxlillash va tadqiqlash sifatida ko'rilishi lozim;

- *tiklash.* Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta`minlash tizimi xavfsizlikning buzilishini tiklash qobiliyatiga ega bo'lishi lozim. Xar doim, qachon axborot xavfsizligini buzishga urinish sodir bo'lganida, tizim ushbu urinish xususidagi axborotni shunday ishlashi lozimki, ushbu urinish ma`lumotlarni uzatish tarmog'ining o'tkazish qobiliyatini va foydalanuvchanligini jiddiy pasayishiga olib kelmasin;

- *moslanuvchanlik.* Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta`minlash tizimiga quyiladigan muxim kontseptual talab-moslanuvchanlik talabi, ya`ni aloqa tarmog'ining tuzilmasi, texnologiyasi va ishlash sharoiti o'zgarganida moslashuv qobiliyati talabidir.

Arxitekturaviy talablar. Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta`minlash tizimi axborot xavfsizligining turli siyosatini madadlashi, ya`ni moslanuvchan bo'lishi lozim. Tizimga quyidagi asosiy xizmatlar kiritilishi mumkin:

- shifrlash kalitlarini va parollarni shakllantirish, saqlash va taqsimlash xizmati;
- shifrlash xizmati;
- foydalanuvchilarni va xabarlarni autentifikatsiyalash xizmati;
- foydalanishni boshqarish xizmati;
- xabarlar yaxlitligini ta`minlash xizmati;
- foydalanuvchanlikni ta`minlash xizmati;
- yetkazilganlikni tasdiqlash xizmati;
- rad qilmaslik xizmati;
- qo'shimcha trafikni shakllantirish xizmati;
- ma`murlash xizmati.

Bu xizmatlarning xar biri axborot xavfsizligini ta`minlash bo'yicha masalalarni mustaqil tarzda u yoki bu ximoya mexanizmlaridan foydalanib yechishi mumkin. Bunda ximoyaning bitta mexanizmi axborot xavfsizligining turli xizmatlarida qo'llanilishi mumkin.

***Boshqarish (ma`murlash) talablari.*** Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ma`murlash xizmati ximoyaning texnik vositalarini to'ldiruvchi ximoya choralarining ma`lum kompleksini o'z ichiga oladi. Bu ximoya choralari buzg'unchining tarmoq axborot xavfsizligiga taxdidni kuchaytirishga qaratilgan u yoki bu ta`sirni o'tkazishini qiyinlashtirish maqsadida mavjud ximoya tizimiga operativ tarzda o'zgartirishlar kiritishga imkon yaratadi.

Ma`murlash xizmatining asosiy vazifalari quyidagilar:

- ximoya xizmati va mexanizmiga zarur axborotni tarqatish;
- ximoya xizmati va mexanizmining ishlashi xususidagi axborotni yig'ish va taxlillash;
- ximoyalanuvchi ob`ektlarni aniqlash;

- xizmat funktsiyalarini samarali amalga oshirish maqsadida ximoya mexanizmlarini kombinatsiyalash;

- ma`lumotlarni uzatish tarmog'ining ishonchli va barqaror ishlashini ta`minlash xizmatlariga javobgar boshqa ma`murlar bilan o'zaro aloqa;

- ma`lumotlarni uzatuvchi tarmoqning buzilgan ishlash jarayonini tiklash.

Xavfsizlik ma`muri ma`murlash xizmatining muxim elementi xisoblanadi. Axborot xavfsizligining xar qanday vositalaridan foydalanilmasin, ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta`minlash sifati ma`murning qobiliyatiga, uning tirishishiga, texnik jixozlanganligiga bog'liq.

Ta`kidlash lozimki, birorta xam real ximoyalangan ma`lumotlarni uzatish tarmog'i mutloq ximoyalangan bo'lmaydi. Shunga qaramasdan ximoyaning adekvat choralari buzg'unchi ta`siri samarasini (zarar keltirish xarajatining kutilayotgan zarar o'lchamiga nisbatini) anchagina pasaytiradi.

Kompyuter tizimlari va tarmoqlarining xavfsizligi deganda, ular me`yoriy ishlash jarayoniga tasodifiy yoki oldindan mo'ljallangan aralashishidan hamda ularning tashkil etuvchilarini o'g'irlashga, o'zgartirishga yoki buzishga bo'lgan intilishlardan himoya qilinganligi tushuniladi.

Axborotga murojaat qilish deganda, axborot bilan tanishib chiqish, uni qayta ishlash, nusxalash, o'zgartirish va yo'qotish tushuniladi.

Axborotga ruxsat etilgan murojaat qilish bu, murojaat qilish cheklanishlariga o'rnatilgan qoidalarni buzmaydigan, axborotga murojaat qilishdir.

Axborotga ruxsat etilmagan murojaat qilish bu murojaat qilish cheklanishlariga o'rnatilgan qoidalarning buzilishi bilan tavsiflanadi.

Berilganlarning maxfiyligi bu berilganlarga taqdim etilgan va ularni himoya qilishni talab etilgan darajasini aniqlaydigan maqomdir.

Tizim sub`ekti tizimning tashkil etuvchisi bo'lib, u ob`ektdan ob`ektga axborot oqishining yoki tizim holatini o'zgartirishni sababchisi bo'lishi mumkin.

Tizim ob`ekti tizimning axborotni saqlaydigan, qabul qiladigan yoki uzatadigan sust tashkil etuvchisidir.

Kompyuter tizimlariga xujum bu tizimning u yoki bu bog'liqligini qidirish va ishlatish ma`nosini bildiradigan, yomon niyatli odam tomonidan bajariladigan harakatdir.

Xavfsiz yoki himoya qilingan tizim xavfsizlik xavflariga muvaffaqiyatli va samarali qarshi turadigan, zarur himoya qilish vositalariga ega bo'lgan tizimdir.

Xavfsizlik siyosati bu himoya qilish vositalarining ishlashini axborot xavfsizligining xavfi berilgan to'plamidan me`yor, qoida va amaliy tavsiyanomalarning yig'indisidir.

Zamonaviy Kompyuter tizimlari va tarmoqlarida axborotni himoya qilish deganda uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotning ishonchliligi va butunligini ta`minlash maqsadida turli xil vosita va usullarni ishlatish, choralarni ko'rish va tadbirlarni o'tkazish tushuniladi.

Axborotni ximoya qilish – bu:

- axborotning fizik butunligini ta`minlash, ya`ni axborot elementlarini xalaqitlarga uchrashi va yo'qolishiga yo'l qo'ymaslik;
- axborot butunligini saqlashda uning elementlarini almashtirishga (modifikatsiyaga) yo'l qo'ymaslik;
- mos vakolatlarga ega bo'lmagan shaxslar yoki jarayonlar tomonidan axborotni ruxsat etilmagan olinishiga yo'l qo'ymaslik;
- egalariga uzatilayotgan resurslar faqatgina tomonlar kelishgan shartlarga mos ravishda ishlatilishiga ishonch hosil qilinishi kerak, demakdir.

Kompyuter tizimlari va tarmoqlarining ishlash tajribasi shuni ko'rsatmoqdaki, axborotga ruxsat etilmagan murojaat qilishni yetarlicha ko'pgina usullari bor:

- ko'rib chiqish;
- berilganlarni nusxalash va almashtirish;
- yo'l va aloqa kanallariga ulanish natijasida yolg'on dastur va xabarlarni kiritish;
- sozlovchi va halokatli dasturlarni ishlatish;
- axborotni uning tashuvchilaridagi qoldiqlarini o'qish;

- elektromagnit nurlanishli va to'lqin xarakterli xabarlarni qabul qilish;
- maxsus dasturli va apparatli so'ndirgichlarni ishlatish.

Axborotni ximoya qilish muammosining dolzarbligi. Axborot xavfsizligini ta`minlash muammosining dolzarbligi va muhimligi quyidagi sabablar bilan shartlangandir:

- zamonaviy Kompyuterlarni ishlatish soddaligi bilan bir vaqtda ularning hisoblash quvvatining keskin oshishi;
- Kompyuter va boshqa avtomatlashtirish vositalari yordamida yig'ilayotgan, saqlanayotgan va qayta ishlanayotgan axborot sig'imining keskin oshishi;
- turli xil vazifali va turli xil tegishli axborotlarni umumiy berilganlar bazasiga mujassamlantirilishi;
- faoliyatning turli sohalarida ishlatishda joylashgan shaxsiy Kompyuterlar narxining o'sishini yuqori sur`atlari;
- hisoblash resurslari va berilganlar bazasiga bevosita murojaat qilish ruxsatiga ega bo'lgan foydalanuvchilar doirasining keskin oshishi;
- axborot xavfsizligining, xattoki minimal talablarini ham qanoatlantirmaydigan dastur vositalarining rivojlanishi;
- tarmoqli texnologiyalarning o'zaro tarqatilishi, lokal va regional tarmoqlarni global tarmoqlarga birlashtirilishi;
- butun dunyoda axborotni qayta ishlash tizimlari xavfsizligining buzilishiga deyarli to'sqinlik qilmaydigan Internet global tarmog'ining rivojlanishi;
- Internet global tarmog'ining ochiqlilik va nazorat qilinmasligi ideologiyasi.

1.2. Aloqa kanallarida ma`lumotlarni ximoyalash usullari

Ma`lumotlarni uzatishni ximoyalash masalasini yechish usullarining uchta asosiy guruxi mavjud: kanalga mo'ljallangan ximoyalash usullari, chekkalararo

ximoyalash usullari va ulanishga mo’ljallangan ximoyalash usullari. Birinchisi xar bir kanal uchun mustaqil ravishda ma`lumotlar oqimini ximoyalashni ta`minlasa, ikkinchisi xar bir xabarni, uni manbadan adresatgacha uzatishda umumiy ximoyalashni ta`minlaydi. Uchinchi usul ikkinchi usulning bir turi xisoblanadi.

Kanalga mo’ljallangan usullar manba va adresatga bog’liq bo’lmagan xolda, aloxida tugunlar orasidagi aloxida aloqa kanali bo’yicha uzatilayotgan xabarlar oqimini ximoyalashni ta`minlaydi. Bu xil ximoyani ta`minlashda buzg’unchining tugunga (paketni kommutatsiyalovchi markazga) qaraganda kanalga ta`sir etish qulayligi faraz qilinadi. Undan tashqari, ma`lumotlarni uzatish tarmog’idagi tugunlarni foydalanuvchi terminallarini ximoyalagandek ximoyalash mumkin emas yoki iqtisod nuqtai nazaridan foydasiz. Ushbu gurux usullarining kamchiligi - qism tarmoq tugunlaridan birining ochilishi tarmoq orqali o’tayotgan xabarlar oqimining talaygina qismini ochilishiga olib kelishi mumkin.

Terminallar va tarmoqlar o’rtasidagi aloqa kanallarini kanalga mo’ljallangan ximoyalash xarajatlari bevosita daxldor taraflar tomonidan qoplansada, ma`lumotlarni uzatish qism tarmog’i ichidagi kanalga mo’ljallangan ximoyalash usullarining umumiy narxi qism tarmoqdan foydalanuvchilarning barchasi o’rtasida xisoblab chiqilishi mumkin.

Chekkalararo ximoyalash usullari xabarlarni manba tugunlari va qabul qiluvchi orasida uzatish jarayonida shunday ximoyalaydiki, manba va adresat orasidagi aloqa kanallaridan birining ochilishi xabarlar oqimining ochilishiga olib kelmaydi. Ushbu usullarning asosiy afzalligi – ulardan foydalanish masalasi aloxida foydalanuvchilar orasida, boshqa foydalanuvchilarni jalb etmasdan, yechilishi mumkin.

Ulanishga mo’ljallangan usullar. Aksariyat qo’llanish soxalarida ma`lumotlarni uzatish tarmog’ini manbadan adresatgacha ulanishni yoki virtual kanalni o’rnatish uchun foydalanuvchiga taqdim etiluvchi muxit sifatida tasavvur etish mumkin. Bunday tasavvur etishda ximoya ulanishga mo’ljallanishi faraz qilinadi, ya`ni, xar bir ulanish yoki virtual kanal aloxida ximoyalanadi. Shunday qilib, ulanishga mo’ljallangan usullar chekkalararo ximoyalash usullarining bir turi

xisoblanadi. Ulanishga mo’ljallangan usullar turli sharoitlarda umumiy ximoyaning yuqori darajasini ta`minlaydi va ximoyaga qo’yiladigan talablar xususidagi foydalanuvchining idrokiga mos keladi. Chunki, ulanishga mo’ljallangan axborot konfidentsialligini ximoyalash usullari asbob - uskunani ximoyalashni, masalan, faqat xabarlar manbaida va qabul qiluvchida axborotdan ruxsatsiz foydalanishdan ximoyalashni ko’zda tutadi. Ayni vaqtda ximoyalashning kanalga mo’ljallangan usullari ruxsatsiz foydalanishdan ximoyalashning ma`lumotlarni uzatish tarmog’idagi xar bir tuguni tomonidan ta`minlanishini talab etishi mumkin. Ammo, ba`zida ikkala usulni qo’llaganda ximoyalashning tejamli darajasiga erishiladi.

Ma`lumotlarni uzatishni ximoyalashning u yoki bu usulidan foydalanishdagi asosiy vazifalar quyidagilar:

- xabarlar mazmunining fosh qilinishini oldini olish;
- xabarlar oqimining taxlillanishini oldini olish;
- xabarlar oqimi xaqiqiyligini buzilganligini aniqlash;
- yolg’on ulanishni aniqlash.

Axborot tizimlari yoki ma`lumotlarni uzatish tarmoqlarida axborot xavfsizligini ta`minlash maqsadida ma`lumotlarni uzatishni ximoyalash usullaridan nafaqat buzg’unchi ta`siri oqibatlarini aniqlashni, balki, agar oqibatlar vaqtincha xarakterga ega bo’lganida, uzilgan (buzilgan) uzatish jarayonini avtomatik tarzda tiklashni talab etish kerak.

Xozirda yuqorida keltirilgan vazifalarning bajarilishini ta`minlovchi ximoyalashning standartlashtirilgan mexanizmlari mavjud emas. Xar bir muayyan xolda ma`lumotlarni uzatish xavfsizligi masalalari axborotlarni kriptografik o’zgartirish usullari, axborotlarni xalaqitlarga bardoshli kodlash usullari, xabarlarning xaqiqiyligini ta`minlovchi usullar, tizimlar ishlashining ishonchliligini, yashovchanligini va barqarorligini ta`minlovchi usullarga asoslangan ximoyalashning turli mexanizmlarini birgalikda ishlatish orqali xal etiladi.

Xabarlar mazmunining fosh qilinishini oldini olishda ximoyalashning kanalga mo'ljallangan xamda ulanishga mo'ljallangan usullaridan foydalanish mumkin.

Kanalli shifrlash aloqa tarmog'ining xar bir kanalida mustaqil tarzda bajarilishi mumkin. Kanalli shifrlashda, odatda, oqimli shifrlash ishlatiladi va tugunlar orasida shifrlangan matn bitlarining uzluksiz oqimi madadlanadi. Tarmoqlarda kommutatsiyalash (marshrutlash) vazifalari faqat tugunlarda bajarilishi sababli, aloqa kanalida paketning sarlavxalari bilan birga axborot qismini xam shifrlash mumkin.

Ammo ma`lumotlar faqat kanalda (kanallar orqali ulangan tugunlarda emas) shifrlanishi sababli barcha oraliq tugunlar ximoyalanishi lozim. Buning ustiga tugunlarni nafaqat fizik ximoyalanishi, balki bu tugunlarning apparat - dasturiy vositalari tomonidan tugunlar orqali o'tuvchi xar bir ulanishdagi axborotni yakkalashi kafolatlanishi zarur.

Chekkalararo shifrlashda marshrutizatorda ishlanuvchi xar bir xabar (sarlavxaning ba`zi ma`lumotlari bundan istisno) yo'l boshida shifrlanadi va belgilangan joyga yetmaguncha rasshifrovka qilinmaydi. Xar bir ulanish uchun o'zining kaliti ishlatilishi mumkin.

Xabarlar oqimini taxlillanishidan ximoyalash, odatda, turli sinflarga mansub xabarlar uzunligi va chastotasining qiymatlarini, manba adreslarini va xabarlar oqimi adreslarini berkitishga yo'naltirilgan. Agar kanalli shifrlash ishlatilsa, tugunlar orasida ma`lumotlar uzatilganida shifrlangan matn bitlarining uzluksiz oqimi o'rnatilishi mumkin. Bu esa chastota qiymatlarini va ulanishning davomligini berkitishga imkon beradi. Bunday yondashishda tarmoqning samarali o'tkazish qobiliyati pasaymaydi, chunki xech qanday qo'shimcha axborot talab etilmaydi. Ammo, tugun ochilsa bu tugun orqali o'tuvchi xabarlarning butun oqimi taxlillash mavzuiga aylanadi.

Ximoyalashning chekkalararo usullaridan foydalanilganda uzatiluvchi xabarlarning xaqiqiy chastotasi va uzunligini berkitish uchun turli uzunlikdagi "bo'sh" xabarlar generatsiyalanishi, xaqiqiy xabar esa bo'sh simvollar bilan

to’ldirilishi mumkin. Qabul qiluvchi begona kengayishlarni va "bo’sh" xabarlarni aniqlashda xabardagi shifrlangan xoshiyadan foydalanishi mumkin.

Aksariyat ilovalarda oqimni taxlillash orqali axborotni chiqarib olish ikkinchi darajali xavf sifatida talqin qilinishi va maxsus qarshi choralar ko’rilmasligi mumkin.

Xabarlar satxida xaqiqiylikni tasdiqlash xabarlarni kechiktirish, ularni yo’q qilish, almashtirib qo’yish yoki qaytalash kabi ta`sirlardan ximoyalashni ta`minlamaydi. Shunga qaramasdan, bunday taxdidlardan ximoyalashning turli usullari mavjud:

- xabarlarni nomerlash. Xar bir xabarni nomerlab, nomerni xabar tarkibiga kiritib, demak, shifrlab uzatish orqali xabarning xaqiqiyligiga ishonch xosil qilish mumkin. Tarmoqning xar bir ob`ekti u bilan aloqada bo’luvchi ob`ektlarning xar biri uchun aloxida sanagichlarga (schetchiklarga) ega bo’lishi lozimligi bu muolajaning kamchiligi xisoblanadi.

- vaqtni belgilash. Qabul qiluvchi xar bir uzatilgan xabarning kuni va vaqtini bilgan xolda uning adekvatligini tekshirishi mumkin. Bunday belgilashning intervali va aniqligi shunday tanlanishi lozimki, bir tomondan xatoli xabarlar, ikkinchi tomondan uzatish kanaliga xos bo’lgan tabiiy kechikish aniqlanishi mumkin bo’lsin.

- tasodifiy sonlardan foydalanish. Vaqtning real masshtabida ikki tomonlama aloqa ishlatilganida qabul qiluvchi jo’natuvchiga xabar jo’natilmasdan oldin tasodifiy son yuboradi. Jo’natuvchi bu sonni shifrlangan xabarga shunday o’rnatadiki, qabul qiluvchi uni tekshirishi mumkin bo’lsin. Shu tarzda yolg’on xabarlar chiqarib tashlanishi mumkin.

- xar bir ulanish uchun aloxida kalitdan foydalanish. Natijada olingan xabarda ulanishning oshkor bo’lmagan identifikatsiyalanishi amalga oshiriladi.

Xabarlar oqimi uzilishini aniqlash masalasini "so’rov-javob" protokolidan foydalanib xal etish mumkin. Bunday protokolning tarkibida ulanishning vaqtinchalik yaxlitligini va maqomini o’rnatuvchi xabarlar juftini almashish muolajasi bo’ladi. Ulanishning xar bir chekkasida "xabar-so’rov" uzatishni vaqti-

vaqti bilan ishga tushiruvchi taymer ishlatiladi va "xabar-so’rov" uzatishga ulanishning boshqa chekkasidan javob olinadi. Xar bir "xabar-so’rov"da uzatuvchi axboroti mavjud bo’lib, bu axborot ulanishdagi xabar yo’qotilishini aniqlashga imkon beradi.

Yolg’on ulanishni aniqlash uchun xar bir chekkadagi "ulanishga javobgar"ning xaqiqiyligini va ulanishning vaqtinchalik yaxlitligini tekshirishga ishonchli asosni ta`minlovchi qarshi choralar ishlab chiqilgan.

Ulanish boshlanishi vaqtida xar bir chekkada ulanishga javobgarning xaqiqiyligini tekshirish keyingi xabarlar oqimining xaqikiyligi xususida qaror qabul qilishga asos xisoblanadi.

Ulanishning vaqtinchalik yaxlitligini tekshirish buzg’unchining oldingi qonuniy ulanish yozuvidan foydalanib, foydalanuvchini xato fikrga solishidan yoki adashtirishidan, ma`lumotlar uzatish jarayonini buzishidan ximoyalaydi.

1.3. Simsiz qurilmalar xavfsizligi muammolari

Simsiz qurilmalarni to’rtta kategoriyaga ajratish mumkin: noutbuklar, cho’ntak Kompyuterlari (PDA), simsiz infratuzilma (ko’priklar, foydalanish nuqtalari va x.) va uyali telefonlar.

Noutbuklar – korporativ simsiz tarmoqlarda va SOHO (Small Office Home Office – kichik va uy ofislari) tarmoqlarida keng tarqalgan qurilma.

Fizik xavfsizlik noutbuklar uchun jiddiy muammo xisoblanadi. Bunday Kompyuterlarni xarid qilishdagi parametrlardan biri - uning o’lchami. Noutbuk qanchalik kichkina bo’lsa, u shunchalik qimmat turadi. Boshqa tarafdan, noutbuk qanchalik kichkina bo’lsa, uni o’g’irlash shunchalik osonlashadi. Shifrlash kalitlarining, masalan, WEP-kalitlar (Wired Equivalent Privacy), dasturiy kalitlar, parollar yoki shaxsiy kalitlarning (PGP, Pretty Good Privace kabilar) yo’qotilishi katta muammo xisoblanadi va uni ilovalar yaratilishi bosqichidayoq xisobga olish zarur. Niyati buzuq odam noutbukni o’z ixtiyoriga olganidan so’ng aksariyat xavfsizlik mexanizmlari buzilishi mumkin.

Noutbuklarning mobilliligi ularning korporativ tarmoqlararo ekranlar (brandmauerlar) bilan ximoyalanmagan boshqa tarmoqlar bilan ulanish extimolligini oshiradi. Bu Internet - ulanishlar, foydalanuvchi tarmoqlar, asbob - uskuna ishlab chiqaruvchilarining tarmog'i yoki raqiblar xam joylanuvchi mexmonxona yoki ko'rgazmalardagi umumfoydalanuvchi tarmoqlar bo'lishi mumkin. Bunday xollarda mobil Kompyuterlarning axborot xavfsizligi xususida jiddiy o'ylanish lozim.

Noutbuklarning fizik saqlanishlarini ta`minlash usullaridan biri-xavfsizlik kabelidan foydalanish. Ushbu kabel noutbukni stolga yoki boshqa yirik predmetga "boylab" qo'yishga mo'ljallangan. Albatta, bu yuz foizlik kafolatni bermaydi, ammo xar xolda o'g'rining anchagina kuch sarf qilishiga to'g'ri keladi.

Noutbuklarning tez - tez o'g'irlanishi sababli, axborotni arxivlashning xavfsizlikni ta`minlashga nisbatan muximligi kam emas. Shifrlash dasturlari fayllar xavfsizligini ta`minlashda yoki qattiq disklarda shifrlangan ma`lumotlar xajmini yaratishda ishlatiladi. Bu ma`lumotlarni rasshifrovka qilish uchun, odatda, parolni kiritish yoki shaxsiy kalitlarni ishlatish talab etiladi. Barcha axborotlarni shifrlangan fayllarda yoki arxivlarda saqlanishi kerakli fayllar to'plamini arxiv uchun nusxalashni yengillashtiradi, chunki ular endi ma`lum joyda joylashgan bo'ladi.

O'g'rilar uchun noutbuklar "birinchi nomerli nishon" ekanligini foydalanuvchilar tushunib yetishlari va ularni qarovsiz qoldirmasliklari zarur. Xatto ofislarda noutbukni kechaga qoldirish mumkin emas, chunki ofisga ko'p kishilar (kompaniya xodimlari, farroshlar, mijozlar) tashrif buyuradilar.

Axborotning chiqib ketishi noutbuk egasining ko'p odamlar to'plangan joylarda xam sodir bo'lishi mumkin. Samolet – kompaniya menedjerlari foydalanadigan odatdagi transport vositasidir. Samoletda qo'shni kreslodagi yo'lovchi noutbuk egasining yelkasi ustidan muxim axborotni o'qib olishi mumkin. Xatto "uy sharoitidagi" noutbuklar xam ximoyalanishi zarur. Bu xolda Kompyuterning ximoyasi server ximoyasidan farqlanmaydi. Juda xam zarur bo'lmagan servislarning o'chirilishi qurilma ishlashini yaxshilaydi.

O’zining dasturiy ta`minotini noutbukka o’rnatgan niyati buzuq odam xavfsizlikning barcha mexanizmlarini chetlab o’tish imkoniyatiga ega bo’ladi. Kompyuterni o’z ixtiyoriga olgan o’g’ri unga o’zining dasturini o’rnatganida uni to’xtatib bo’lmaydi. BIOSda (Basic InputG’Output System-kiritishG’chiqarishning bazaviy tizimi) va qattiq diskda o’rnatilgan parollar o’g’irlangan noutbukdan foydalanishga to’sqinlik qilishi mumkin.

Ushbu barcha vositalar, afsuski, tajribali xaker uchun to’siq bo’laolmaydi.

Cho’ntak Kompyuterlari. PDA(Personal Digital Assistans – "shaxsiy raqamli yordamchilar")ning ko’pgina xillaridan simsiz ilovalar bilan ishlashda foydalaniladi. Maxsus qurilgan PDAlarda tibbiyot, sanoat yoki aviatsiya ilovalari ishga tushiriladi. Cho’ntak Kompyuterlari xam mavjud bo’lib, ularda simsiz aloqa uchun o’rnatilgan kartochka, shtrix kodlarning skaneri, xizmat muddati uzoq bo’lgan batareyalar yoki magnit xoshiyali kartalarni o’quvchi qurilma kabi qo’shimcha qurilmalar bilan birgalikda Palm OS yoki Windows SE operatsion tizim o’rnatilgan. Bunday Kompyuterlardan foydalanish uchun maxsus texnik tayyorgarlik talab etilmaydi. Shunga o’xshash qurilmalarni yoki ilovalarni ximoyalash ayniqsa murakkab masala xisoblanadi.

PDAdan foydalanishga xoxish bildirgan xujum qiluvchi uchun undagi axborot kiritish mexanizmlarining barchasi nishon xisoblanadi. Undan tashqari, aksariyat cho’ntak Kompyuterlari shunday ishlab chiqilganki, ularni ishlab chiquvchilari uchun ilovalardagi xatoliklarni osongina aniqlash yo’llari ta`minlangan. Xatoliklarni aniqlashda ishlatiluvchi interfeyslar niyati buzuq odamlar uchun xaqiqiy "teshik" xizmatini o’tashi mumkin.

Cho’ntak Kompyuteri ishlaydigan axborotni ximoyalash uchun axborotni cho’ntak Kompyuterida emas, balki ma`lumotlarning xavfsiz rezerv bazasida saqlash lozim. Yana bir variant – JAVA tili ilovasidan yoki foydalanuvchi uchun maxsus yaratilgan ilovalardan foydalanish. Bu xolda axborot qurilmada saqlanmaydi, ammo, PDAning displeyida akslantiriladi. Boshqacha aytganda, simsiz ilovalardan faqat simsiz tarmoqdan foydalanish mavjud bo’lgan joylarda foydalanish mumkin.

Aksariyat PDAlarda parol yordamida blokirovka va razblokirovka qilish imkoniyati mavjud. Bu usullarga butunlay ishonmaslik lozim, ammo ular niyati buzuq odamlarni vaqtincha to’xtatib turishi mumkin. Undan tashqari PDAni blokirovka qilish tizimi qurilmadagi ilovalardan yoki axborotdan niyati buzuq odamlarning foydalanishni qiyinlashtiradi. PDAning zarur bo’lmagan barcha funktsiyalarini o’chirib quyish lozim, chunki xar bir o’chirilgan kiritish mexanizmi bo’lishi mumkin bo’lgan xujumlar sonini kamaytiradi.

Cho’ntak Kompyuterida muxim axborotni saqlash uchun shifrlashni qo’llash va unga qo’shimcha sifatida manbani ulash va ekranni blokirovka qilish uchun parollar o’rnatish tavsiya etiladi.

Simsiz infratuzilma. Simsiz infratuzilma qurilmalari odatda odamlar yig’ilgan yerda joylashtiriladi. Ularga kafelar, aeroportlar, korporativ tadbirlarni o’tkazish joylari va x. kiradi. Turli xil odamlar EAP(Extensible Authentification Protocol – autentifkatsiyalashning kengaytiriluvchi protokoli) yoki WEP kabi xavfsizlik vositalarini ishdan chiqarish yoki tarmoqqa suqilib kirish uchun tarmoq konfiguratsiyasi xususidagi axborotni qo’lga kiritish maqsadida ushbu komponentlardan foydalanishni xoxlashlari mumkin.

Simsiz infratuzilma qurilmalarida tarmoqni boshqarish funktsiyalarining xavfsizligini ta`minlash uchun ulardan foydalanishda SSh, SSL (Secure Sockets Layer) yoki SNMP3 (Simple Network Management Protocol 3 – tarmoqni oddiy boshqarish protokoli, 3-versiya) kabi xavfsiz protokollardan foydalanish lozim. Undan tashqari telnet, HTTP dagi to’g’ri matn, va SNMP (birinchi versiya) kabi xavfsizlik yetarli darajasini madadlamaydigan protokollar o’chirilishi lozim. Xavfsiz boshqarishni ta`minlash iloji bo’lmasa, foydalanishning ba`zi bir nuqtalarini ketma-ket portlar orqali boshqarish mantiqan to’g’ri xisoblanadi. Foydalanish nuqtalarini yuqoriga qo’l yetmaydigan joyga maxkamlab qo’yish ham ularni o’g’irlanishdan saqlaydi.

Uyali telefonlar. Uyali telefonlar uchun xavfsizlik muloxazalari noutbuk va PDAlarga nisbatan keltirilgan muloxazalarga o’xshash. Qurilmalarning o’zi va

mos dasturiy ta`minot uchun xavfsizlik muammosi xam xech nimasi bilan farq qilmaydi.

Uyali telefonlar xam boshqa simsiz qurilmalarga bo'ladigan xujumlarga duchor bo'ladilar. Odatda buferning to'lib - toshishi, qator formatiga xujumlash, grammatik xatoliklar ishlatiladi, natijada xujum qiluvchi o'g'irlangan qurilmada o'zining dasturini ishga tushirishga erishadi. Misol sifatida SMSning qisqa xabarlarini ko'rsatish mumkin. O'zining telefoni orqali SMS jo'natgan foydalanuvchiga xujumga duchor bo'lishi xavfi tug'iladi. Bu xujum natijasida xizmat qilish to'xtatiladi yoki foydalanuvchi terminalida begonaning komandalari bajariladi.

Undan tashqari SIM-kartalarni (Subscriber Idenity Module – abonent identifkatsiyasi moduli) ishlab chiqaruvchilari qurilmalariga uyali telefonga simsiz interfeys orqali yuklanilishi ruxsat etiladigan qo'shimcha funktsiyalarni kirita boshladilar. Misol tariqasida Sim Toolkit va MEXEni ko'rsatish mumkin. Zararli ilovalarni boshqa foydalanuvchiga uzatishni oldini oluvchi usullar tashqi xujumlarga duchor bo'ladi. Bunday ilovalarning moxiyati shundaki u niyati buzuq odamga foydanuvchining adres kitobini yoki telefondagi butun SMS ro'yxatini uzatishi mumkin. Ba`zi yechimlar DES standarti asosida ishlaydi, ammo xuddi shunday DES-kalitlar xar bir SIM-kartalar uchun ishlatiladi.

Terminallar uchun parol yoki PIN-kodlarni ishlatish tavsiya etiladi. GSM(Global System for Mobile Communications – mobil kommunikatsiyalarning global tizimi) tarmoqlarida ishlovchi telefonlar xavfsizligini ta`minlashda SIM PIN kerak bo'ladi. Bu funktsiyadan maksimal foydalanish uchun barcha bo'lishi mumkin bo'lgan PINlardan foydalanish xamda IMEI (International Mobile Equipment Identity – mobil qurilmaning xarqaro nomeri)ning ishonchli joyda yozilishi tavsiya etiladi.

Muxim axborotni uzatish uchun terminaldan foydalanishida axborotni albatta shifrlash zarur. Kredit kartochkalar nomerlarini yoki boshqa shaxsiy axborotni uzatish uchun albatta SSL-ximoyali WTLS-ulanish xizmatidan foydalanish zarur. Undan tashqari GSM ichidagi algoritmlarga bo'ladigan

aksariyat xujumlar niyati buzuq odamga foydalanuvchining telefon nomerini o’ylab chiqarishga (klonirovka) imkon beradi. Bu xujumlar odatda telefon mavjudligini talab qiladi, shu sababli telefonni xavfsiz joyda saqlash, yo’qotilgan yoki o’g’irlangan xolda tezlik bilan operatorga xabar berish lozim.

XULOSA

Ushbu bo’limda ma`lumot uzatish tarmog’ida axborotni ximoya qilish ko’rib chiqilgan. Asosan ma`lumotlarni uzatish tarmoqlarida axborot ximoyasini ta`minlash, boshqarish, arxitekturaviy, talablari keltirilgan. Asosiy tushuncha va atamalari, axborotni ximoya qilish talablari, ruxsat etilmagan murojaat qilish usullari, va axborotni ximoya qilish dolzarbligi batafsil keltirilgan.

Aloqa kanallarida ma`lumotlarni ximoyalash, chekkalararo ximoyalash, ulanishga mo’ljallangan usullari va bu usullardan foydalanishdagi asosiy vazifalari keltirilgan.

Ma`lumot uzatishda simsiz aloqadan foydalanish telekommunikatsiya soxasining rivojlanishidan darak beradi. Shulardan biri simsiz qurilmalarning xavfsizligini ta`minlashdir. Noutbuklar, cho’ntak Kompyuterlari, simsiz infratuzilma va uyali telefonlar shular jumlasiga kiradi.

2. AXBOROT XAVFSIZLIGIGA TAXDIDLAR

2.1. Axborot-kommunikatsion tizimlar va tarmoqlarda taxdidlar va zaifliklar

Tarmoq texnologiyalari rivojining boshlang'ich bosqichida viruslar va Kompyuter xujumlarining boshqa turlari ta`siridagi zarar kam edi, chunki u davrda dunyo iqtisodining axborot texnologiyalariga bog'liqligi katta emas edi. Xozirda, xujumlar sonining doimo o'sishi xamda biznesning axborotdan foydalanish va almashishning elektron vositalariga bog'liqligi sharoitida mashina vaqtining yo'qolishiga olib keluvchi xatto ozgina xujumdan kelgan zarar juda katta raqamlar orqali xisoblanadi. Misol tariqasida keltirish mumkinki, faqat 2003 yilning birinchi choragida dunyo miqyosidagi yo'qotishlar 2002 yildagi barcha yo'qotishlar yig'indisining 50%ini tashkil etgan, yoki bo'lmasa 2006 yilning o'zida Rossiya Federeatsiyasida 14 mingdan ortiq Kompyuter jinoyatchiligi xolatlari qayd etilgan.

Korporativ tarmoqlarda ishlanadigan axborot, ayniqsa, zaif bo'ladi. Xozirda ruxsatsiz foydalanishga yoki axborotni modifikatsiyalashga, yolg'on axborotning muomalaga kirishi imkonining jiddiy oshishiga quyidagilar sabab bo'ladi:

- Kompyuterda ishlanadigan, uzatiladigan va saqlanadigan axborot xajmining oshishi;
- ma`lumotlar bazasida muximlik va maxfiylik darajasi turli bo'lgan axborotlarning to'planishi;
- ma`lumotlar bazasida saqlanayotgan axborotdan va xisoblash tarmoq resurlaridan foydalanuvchilar doirasining kengayishi;
- masofadagi ishchi joylar soninig oshishi;
- foydalanuvchilarni bog'lash uchun Internet global tarmog'ini va aloqaning turli kanallarini keng ishlatish;
- foydaluvchilar Kompyuterlari o'rtasida axborot almashinuvining avtomatlashtirilishi.

Axborot xavfsizligiga taxdid deganda axborotning buzilishi yoki yo’qotilishi xavfiga olib keluvchi ximoyalanuvchi ob`ektga qarshi qilingan xarakatlar tushuniladi. Oldindan shuni aytish mumkinki, so’z barcha axborot xususida emas, balki uning faqat, mulk egasi fikricha, kommertsiya qiymatiga ega bo’lgan qismi xususida ketyapti.

Xavfsizlikka taxdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashqarisida (tashqi manba) bo’lishi mumkin. Bunday ajratish to’g’ri, chunki bitta taxdid uchun (masalan, o’g’irlash) tashqi va ichki manbalarga qarshi xarakat usullari turlicha bo’ladi. Bo’lishi mumkin bo’lgan taxdidlarni xamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta`minlovchi eng samarali vositalarni tanlash uchun zarur xisoblanadi.

Tez - tez bo’ladigan va xavfli (zarar o’lchami nuqtai nazaridan) taxdidlarga foydalanuvchilarning, operatorlarning, ma`murlarning va korporativ axborot tizimlariga xizmat ko’rsatuvchi boshqa shaxslarning atayin qilmagan xatoliklari kiradi. Ba`zida bunday xatoliklar (noto’g’ri kiritilgan ma`lumotlar, dasturdagi xatoliklar sabab bo’lgan tizimning to’xtashi yoki bo’zilishi) to’g’ridan to’g’ri zararga olib keladi. Ba`zida ular niyati buzuq odamlar foydalanishi mumkin bo’lgan nozik joylarni paydo bo’lishiga sabab bo’ladi. Global axborot tarmog’ida ishlash ushbu omilning yetarlicha dolzarb qiladi. Bunda zarar manbai tashkilotning foydalanuvchisi xam, tarmoq foydalanuvchisi xam bo’lishi mumkin, oxirgisi ayniqsa xavfli.

Zarar o’lchami bo’yicha ikkinchi o’rinni o’g’irlashlar va soxtalashtirishlar egallaydi. Tekshirilgan xolatlarning aksariyatida ishlash rejimlari va ximoyalash choralari bilan a`lo darajada tanish bo’lgan tashkilot shtatidagi xodimlar aybdor bo’lib chiqdilar. Global tarmoqlar bilan bog’langan quvvatli axborot kanalining mavjudligida, uning ishlashi ustidan yetarlicha nazorat yo’qligi bunday faoliyatga qo’shimcha imkon yaratadi.

Xafa bo’lgan xodimlar (xatto sobiqlari) tashkilotdagi tartib bilan tanish va juda samara bilan ziyon yetkazishlari mumkin. Xodim ishdan bo’shaganida uning axborot resurslaridan foydalanish xuquqi bekor qilinishi nazoratga olinishi shart.

Xozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo'lishi mumkin bo'lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo'lib tuyulmasa xam, Internetda ishlash tajribasi ko'rsatadiki, qariyb xar bir Internet - server kuniga bir necha marta suqilib kirish urinishlariga duchor bo'lar ekan. Xavf-xatarlar taxlil qilinganida tashkilot korporativ yoki lokal tarmog'i Kompyuterlarining xujumlarga qarshi turishi yoki bo'lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun yetarlicha ximoyalanmaganligini xisobga olish zarur. Masalan, axborot tizimlarini ximoyalash Agentligining (AQSh) testlari ko'rsatadiki, 88% Kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan masofadan foydalanish xollari aloxida ko'rilishi lozim.

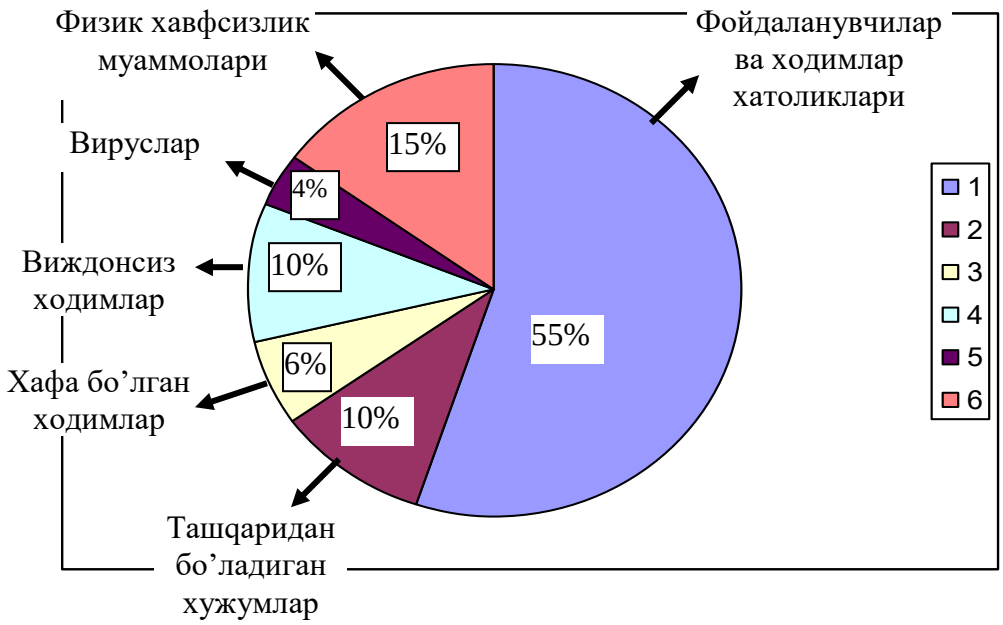
Ximoya siyosatini tuzishdan avval tashkilotda Kompyuter muxiti duchor bo'ladigan xavf - xatar baxolanishi va zarur choralar ko'rilishi zarur. Ravshanki, ximoyaga taxdidni nazoratlash va zarur choralarni ko'rish uchun tashkilotning sarf - xarajati tashkilotda aktivlar va resurslarni ximoyalash bo'yicha xech qanday choralar ko'rilmaganida kutiladigan yo'qotishlardan oshib ketmasligi shart.

Umuman olganda, tashkilotning Kompyuter muxiti ikki xil xavf-xatarga duchor bo'ladi:

1. Ma`lumotlarni yo'qotilishi yoki o'zgartirilishi.
2. Servisning to'xtatilishi.

Taxdidlarning manbalarini aniqlash oson emas. Ular niyati buzuq odamlarning bostirib kirishidan to Kompyuter viruslarigacha turlanishi mumkin.

Bunda inson xatoliklari xavfsizlikka jiddiy taxdid xisoblanadi. 2.1-rasmda korporativ axborot tizimida xavfsizlikning buzilish manbalari bo'yicha statistik ma`lumotlarni tasvirlovchi aylanma diagramma keltirilgan.



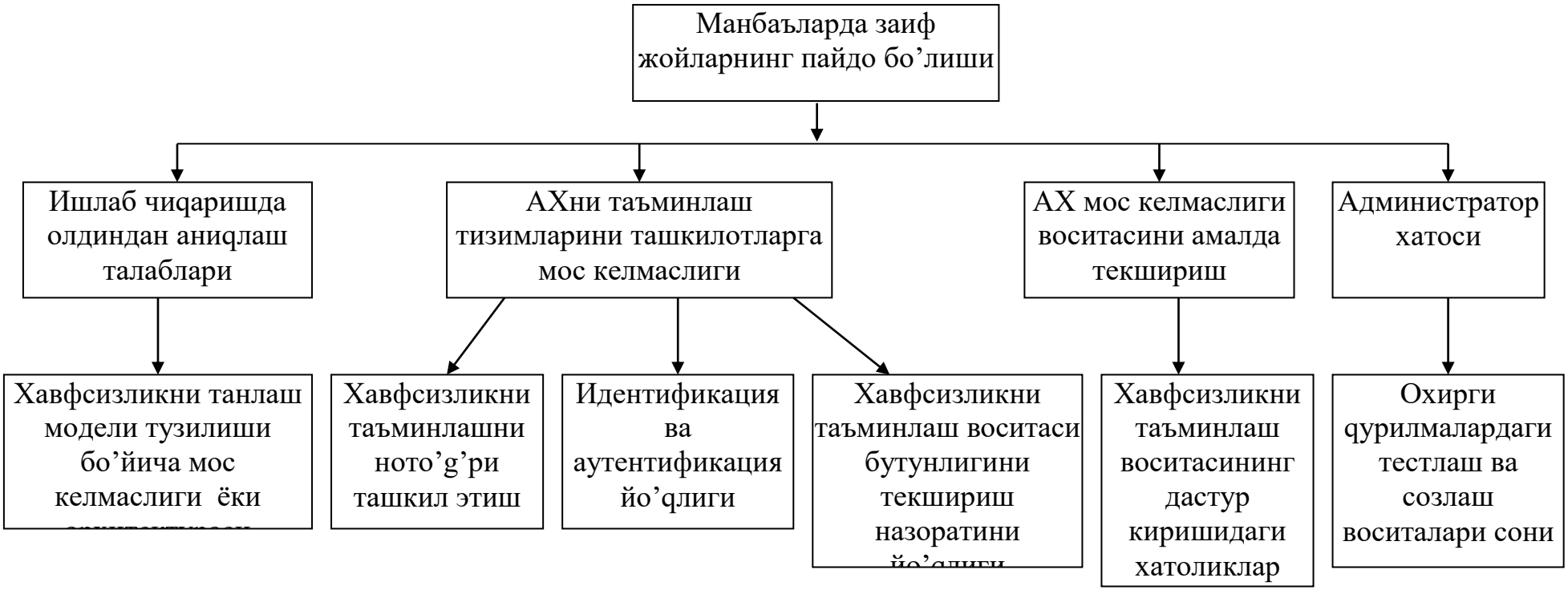
2.1-rasm. Xavfsizlikning buzilish manbalari

2.1.-rasmda keltirilgan statistik ma`lumotlar tashkilot ma`muriyatiga va xodimlariga korporativ tarmoq va tizimi xavfsizligiga taxdidlarni samarali kamaytirish uchun xarakatlarni qaerga yo'naltirishlari zarurligini aytib berishi mumkin. Albatta, fizik xavfsizlik muammolari bilan shug'ullanish va inson xatoliklarining xavfsizlikka salbiy ta`sirini kamaytirish bo'yicha choralar ko'rilishi zarur. Shu bilan bir qatorda korporativ tarmoq va tizimga xam tashqaridan, xam ichkaridan bo'ladigan xujumlarni oldini olish bo'yicha tarmoq xavfsizligi masalasini yechishga jiddiy e`tiborni qaratish zarur.

Ataylab qilingan	Aktiv	buzuvchi dasturiy vositalari	troyan oti
			viruslar
	tizimga bildirmasdan kirish		
	Passiv	yashirin kanaldagi ma`lumotlar oqimi	xotiradan foydalanish
			vaqtdan foydalanish
Tasodifiy	Nazorat o’tkazishdagi ko’rsatkichlar xatolari		
	Domen aniqlashdagi xatolar		
	Bitta ob`ekt uchun xar-xil turdagi nomlardan foydalanish va ketma-ketliklar xatolari		
	Identifikatsiya va audentifikatsiya xatolari		
	ob`ektlar chegaralarini tekshirishdagi xatolar		

Axborot tizimida zaif joylarni joylashish klassifikatsiyasi

Dasturiy ta`minot	operatsion tizim
	dasturlash xizmatlari
	amaliy daturlash
	jixozli (apparatli) ta`minot



2.2 – Manba`larda zaif joylarning paydo bo’lishi

Zaif joylarni satx bo’yicha paydo bo’lish klassifikatsiyasi

Zaif joylarni paydo bo’lishi va joriy qilishdagi satx xatolari	ishlab chiqarish bosqichi	spetsifikatsiyalash va talablardagi xatolar
		chiqish dasturiy tekstlaridagi xatolar
		bajaruvchi koddagi xatolar
		kuzatish jarayonida
		ekspluatatsiya jarayonida

Kompyuter tizimlari va tarmoqlarida (KT va T) axborotni ishonchli himoya qilish, agar havf paydo bo’lishi mumkin bo’lgan tizimning barcha ob`ektlari va elementlarida ishonchli bo’lsagina, samarali bo’lishi mumkin. Shu munosabat bilan himoya qilish vositalarini yaratish uchun havf tabiatini, shakllarini va ularning mumkin bo’lgan paydo bo’lish va amalga oshirish yo’llari, ob`ektlar va elementlar ro’yxatini aniqlash muhimdir. Ular, bir tomondan, axborotning himoyalanganligini buzish maqsadida havflarga duch kelishi mumkin, boshqa tomondan esa, axborotni samarali himoya qilishni tashkil etishi mumkin.

Himoya qilish ob`ekti deganda, tizimning shunday tashkil etuvchisi tushuniladiki, unda himoya qilinishi mumkin bo’lgan axborot joylashgan yoki joylashishi mumkin.

Kompyuter tizimlarini axborotni himoya hilish ob`ektlari sifatida quyidagilarni ajratish mumkin:

- foydalanuvchilarning terminallari (shaxsiy Kompyuterlar tarmoqning ishchi stantsiyalari);
- tarmoq majburiyatining terminali yoki guruhli abonentlik tuguni;
- aloka tuguni;
- axborotni aks ettirish vositalari;
- mashina vali (Kompyuterli yoki displeyli) va axborot tashuvchilari omborxonasi;
- tashqi aloqa kanallari va tarmoqdagi jihozlar;

- axborotni yig’uvchilar va tashuvchilar.

Himoya qilish elementi deganda esa, himoya qilinishi kerak bo’lgan ma`lumotlarni o’z ichiga olgan berilganlar to’plami tushuniladi.

Yuqorida keltirilgan ta`rifga mos ravishda himoya qilish elementlari sifatida himoya qilish ob`ektlaridagi axborot bloklari (miqdorlar, to’plamlar, oqimlar, bazalar va boshqa) qatnashishi mumkin, xususan:

- Kompyuterning asosiy xotirasidagi berilganlar va dasturlar;
- tashqi mashina tashuvchisidagi (qattiq yoki egiluvchan disklardagi) berilganlar va dasturlar;
- shaxsiy Kompyuterlar avtonom yoki tarmoqda ishlatilganda printerga chiqarilayotgan ma`lumotlar;
- monitor ekranida aks ettirilayotgan ma`lumotlar;
- aloqa kanallari bo’yicha uzatilayotgan ma`lumotlar paketlari;
- nusxa olish – ko’paytirish jihozlari yordamida ko’paytirilayotgan ma`lumotlar;
- foydalanuvchi tomonidan ro’yhatga olingan parol va prioritetlar vazifalarining jurnallari;
- masalalar to’plami bilan ishlash bo’yicha xizmatga doir yo’riqnomalar;
- berilganlar va dastur ta`minoti arxivlari;
- tarmoqli operatsion tizimlar;
- tarmoqli ishchi tugunlar va qism stantsiyalar.

Ruxsatsiz kirishning mumkin bo’lgan asosiy usullariga quyidagilar kiradi:

1. kabel quduqlari, taqsimlovchi korobka, taqsimlovchi shkaflar, kross qurilmasi vaboshqalar;
2. interfeyslar, portlar, tizimlar;
3. xalqaro va shaxarlararo tutashgan joylar va boshqalar;
4. tarmoq analizatorlari protokollari va tarmoq teserlari;
5. diagnostika va boshqarish, nazorat, texnologik o’lchov pul tlari;

6. apparatura ichki montaji;

7. apparat vositalarining tizimi orasidagi aloqa liniyalari.

Axborotga shtatli murojaat qilish vositalari quyidagilardan iborat:

1. terminal foydalanuvchilari;

2. terminallar administrator (boshqaruvchi) tizimlari;

3. funktsional nazorat terminal operatori;

4. axborotni aks ettirish vositasi;

5. ma`lumot tashuvchi;

6. telelekommunikatsiya tashqi kanallari.

2.2. Kompyuter jinoyatchiligining taxlili

Kompyuter jinoyatchiligi statistikasi taxlil etilsa qayg'uli manzaraga ega bo'lamiz. Kompyuter jinoyatchiligi yetkazgan zararni narkotik moddalar va qurollarning noqonuniy aylanishidan olingan foydaga qiyoslash mumkin. Faqat AQShda "elektron jinoyatchilar" yetkazgan xar yilgi zarar qariyb 100 mld. dollarni tashkil etar ekan.

Yaqin kelajakda jinoiy faoliyatning bu turi daromadliligi, pul mablag'larining aylanishi va unda ishtirok etuvchi odamlar soni bo'yicha yaqin vaqtlargacha noqonuniy faoliyat orasida daromadligi bilan birinchi o'rinni egallagan noqonuniy biznesning uch turidan uzib ketish extimolligi katta. Bu noqonuniy bizneslar - narkotik moddalar, qurol va kam uchraydigan yovvoyi xayvonlar bilan savdo qilish.

Davlat va xususiy kompaniyalar faoliyatining sotsiologik tadqiqi ma`lumotlariga qaraganda XXI asrning birinchi yillarida iqtisodiy soxadagi jinoyatchilik bank va boshqa tizimlarning axborot-kommunikatsion komplekslariga bo'lishi mumkin bo'lgan g'arazli iqtisodiy xarakatlarga qaratilgan bo'ladi.

Kredit - moliya soxasidagi Kompyuter jinoyatchiligining soni muttasil o'sib bormoqda. Masalan onlayn magazinlarida 25%gacha qalloblik to'lov amallari qayd

etilgan. Shunga qaramasdan G’arb davlatlarida elektron tijoratning-yuqori daromadli zamonaviy biznesning faol rivojlanishi ko’zga tashlanmoqda. Ma`lumki, bu soxa rivojlanishi bilan parallel ravishda "virtual" qalloblarning xam daromadi oshadi. Qalloblar endi yakka xolda xarakat qilmaydilar, ular puxtalik bilan tayyorlangan, yaxshi texnik va dasturiy qurollangan jinoiy guruxlar bilan, bank xizmatchilarining o’zlari ishtirokida ishlaydilar.

Xavfsizlik soxasidagi mutaxassislarning ko’rsatishicha bunday jinoyatchilarning ulushi 70%ni tashkil etadi. "Virtual" o’g’ri o’zining xamkasbi - oddiy bosqinchiga nisbatan ko’p topadi. Undan tashqari "virtual" jinoyatchilar uyidan chiqmasdan xarakat qiladilar. Foydalanishning elektron vositalarini ishlatib qilingan o’g’rilik zararining o’rtacha ko’rsatkichi faqat AQShda bankni qurolli bosqinchilikdan kelgan zararning o’rtacha statistik zararidan 6-7 marta katta.

Bank xizmati va moliya amallari soxasidagi turli xil qalloblik natijasida yo’qotishlar 1989 yili 800 mln. dollardan 1997 yili – 100 mlrd. dollarga yetgan. Bu ko’rsatkichlar o’sayapti, aslida yuqorida keltirilgan ma`lumotlardan bir tartibga oshishi mumkin. Chunki ko’p yo’qotishlar aniqlanmaydi yoki e`lon qilinmaydi. O’ziga xos "*indamaslik siyosati*"ni tizim ma`murlarining o’zining tarmog’idan ruxsatsiz foydalanganlik tafsilotini, bu noxush xodisaning takrorlanishidan qo’rqib va o’zining ximoya usulini oshkor etmaslik vajida muxokama etishni xoxlamasliklari bilan tushunish mumkin.

Kompyuter ishlatiladigan inson faoliyatining boshqa soxalarida xam vaziyat yaxshi emas. Yildan-yilga xuquqni muxofaza qiluvchi organlariga Kompyuter jinoyatchiligi xususidagi murojaatlar oshib bormoqda.

Barcha mutaxassislar viruslarning tarqalishi bilan bir qatorda tashqi xujumlarning keskin oshganligini e`tirof etmoqdalar. Ko’rinib turibdiki, Kompyuter jinoyatchiligi natijasida zarar qat`iy ortmoqda. Ammo Kompyuter jinoyatchiligi ko’pincha "virtual" qalloblar tomonidan amalga oshiriladi deyish xaqiqatga to’g’ri kelmaydi. Xozircha Kompyuter tarmoqlariga suqilib kirish xavfi xar biri o’zining usuliga ega bo’lgan xakerlar, krakerlar va Kompyuter qaroqchilari tomonidan kelmoqda.

Xakerlar, boshqa Kompyuter qaroqchilaridan farqli xolda, ba`zida, oldindan, maqtanish maqsadida Kompyuter egalariga ularning tizimiga kirish niyatlari borligini bildirib qo'yadilar. Muvaffaqiyatlari xususida Internet saytlarida xabar beradilar. Bunda xaker musobaqalashuv niyatida kirgan Kompyuterlariga zarar yetkazmaydi.

Krakerlar (cracker) – elektron "o'g'rilar" manfaat maqsadida dasturlarni buzishga ixtisoslashganlar. Buning uchun ular Internet tarmog'i bo'yicha tarqatiluvchi buzishning tayyor dasturlaridan foydalanadilar.

Kompyuter qaroqchilari – raqobat qiluvchi firmalar va xatto ajnabiy maxsus xizmatlari buyurtmasi bo'yicha axborotni o'g'irlovchi firma va kompaniyalarning yuqori malakali mutaxassislari. Undan tashqari ular begona bank schetidan pul mablag'larini o'g'irlash bilan xam shug'ullanadilar.

Ba`zi "mutaxassislar" jiddiy gurux tashkil qiladilar, chunki bunday kriminal biznes o'ta daromadlidir. Bu esa tez orada, "virtual" jinoyatning zarari jinoyat biznesining an`anaviy xilidagi zarardan bir tartibga (agar ko'p bo'lmasa) oshishiga sabab bo'ladi. Xozircha bunday taxdidni betaraflashtirishning samarali usullari mavjud emas.

2.3. Tarmoqdagi axborotga bo'ladigan namunaviy xujumlar

Barcha xujumlar Internet ishlashi printsiplarining qandaydir chegaralangan soniga asoslanganligi sababli masofadan bo'ladigan namunaviy xujumlarni ajratish va ularga qarshi qandaydir kompleks choralarni tavsiya etish mumkin. Bu choralar, xaqiqatan, tarmoq xavfsizligini ta`minlaydi.

Internet protokollarining mukammal emasligi sababali tarmoqdagi axborotga masofadan bo'ladigan asosiy namunaviy xujumlar quyidagilar:

- tarmoq trafigini taxlillash;
- tarmoqning yolg'on ob yektini kiritish;
- yolg'on marshrutni kiritish;
- xizmat qilishdan voz kechishga undaydigan xujumlar.

Tarmoq trafigini taxlillash. Serverdan Internet tarmog'i bazaviy protokollari FTP (File Transfer Protocol) va TELNET (Virtual terminal protokoli) bo'yicha foydalanish uchun foydalanuvchi *identifikatsiya* va *autentifikatsiya* muolajalarini o'tishi lozim. Foydalanuvchini identifikatsiyalashda axborot sifatida uning identifikatori (ismi) ishlatilsa, autentifikatsiyalash uchun *parol* ishlatiladi. FTP va TELNET protokollarining xususiyati shundaki, foydaluvchilarning paroli va identifikatori tarmoq orqali ochiq, shifrlanmagan ko'rinishda uzatiladi. Demak, Internet xostlaridan foydalanish uchun foydalanuvchining ismi va parolini bilish kifoya.

Axborot almashinuvida Internetning masofadagi ikkita tuguni almashinuv axborotini *paketlarga* bo'lishadi. Paketlar aloqa kanallari orqali uzatiladi va shu paytda ushlab qolinishi mumkin.

FTP va TELNET protokollarining taxlili ko'rsatadiki, TELNET parolni simvollarga ajratadi va parolning xar bir simvolini mos paketga joylashtirib bittalab uzatadi, FTP esa, aksincha, parolni butunlayicha bitta paketda uzatadi. Parollar shifrlanmaganligi sababli paketlarning maxsus skaner-dasturlari yordamida foydalanuvchining ismi va paroli bo'lgan paketni ajratib olish mumkin. Xuddi shu sababli, xozirda ommaviy tus olgan ICQ dasturi xam ishonchli emas. ICQning protokollari va axborotlarni saqlash, uzatish formatlari ma`lum va demak, uning trafigi ushlab qolinishi va ochilishi mumkin.

Asosiy muammo almashinuv protokolida. Bazaviy tatbiqiy prokollarning TCPG'IP oilasi ancha oldin (60 yillarning oxiri va 80-yillarning boshi) ishlab chiqilgan va undan beri umuman o'zgartirilmagan. ¡tgan davr mobaynida taqsimlangan tarmoq xavfsizligini ta`minlashga yondashish jiddiy o'zgardi. Tarmoq ulanishlarini ximoyalashga va trafikni shifrlashga imkon beruvchi axborot almashinuvining turli protokollari ishlab chiqildi. Ammo bu protokollar eskilarining o'rnini olmadi (SSL bundan istisno) va standart maqomiga ega bo'lmadi. Bu protokollarining standart bo'lishi uchun esa tarmoqdan foydalanuvchilarning barchasi ularga o'tishlari lozim. Ammo, Internetda tarmoqni

markazlashgan boshqarish bo’lmaganligi sababli bu jarayon yana ko’p yillar davom etishi mumkin.

***Tarmoqning yolg’on ob`ektini kiritish.*** Xar qanday taqsimlangan tarmoqda qidirish va adreslash kabi "nozik joylari" mavjud. Ushbu jarayonlar kechishida tarmoqning yolg’on ob`ektini (odatda bu yolg’on xost) kiritish imkoniyati tug’iladi. Yolg’on ob yektning kiritilishi natijasida adresatga uzatmoqchi bo’lgan barcha axborot aslida niyati buzuq odamga tegadi. Taxminan buni tizimingizga, odatda elektron pochtani jo’natishda foydalanadigan provayderingiz serveri adresi yordamida kirishga kimdir uddasidan chiqqani kabi tasavvur etish mumkin. Bu xolda niyati buzuq odam unchalik qiynalmasdan elektron xat-xabaringizni egallashi, mumkin, siz esa xatto undan shubxalanmasdan o’zingiz barcha elektron pochtangizni jo’natgan bo’lar edingiz.

Qandaydir xostga murojaat etilganida adreslarni maxsus o’zgartirishlar amalga oshiriladi (IP-adresdan tarmoq adapteri yoki marshrutizatorining fizik adresi aniqlanadi). Internetda bu muammoni yechishda ARP(Adress Resolution Protocol) protokolidan foydalaniladi. Bu quyidagicha amalga oshiriladi: tarmoq resurslariga birinchi murojaat etilganida xost keng ko’lamli ARP-so’rovni jo’natadi. Bu so’rovni tarmoqning berilgan segmentidagi barcha stantsiyalar qabul qiladi. So’rovni qabul qilib, xost so’rov yuborgan xost xususidagi axborotni o’zining ARP-jadvaliga kiritadi, so’ngra unga o’zining Ethernet-adresi bo’lgan ARP-javobni jo’natadi. Agar bu segmentda bunday xost bo’lmasa, tarmoqning boshqa segmentlariga murojaatga imkon beruvchi marshrutizatorga murojaat qilinadi. Agar foydalanuvchi va niyati buzuq odam bir segmentda bo’lsa, ARP-so’rovni ushlab qolish va yolg’on ARP-javobni yo’llash mumkin bo’ladi. Bu usulning ta`siri faqat bitta segment bilan chegaralanganligi tasalli sifatida xizmat qilishi mumkin.

ARP bilan bo’lgan xolga o’xshab DNS-so’rovni ushlab qolish yo’li bilan Internet tarmog’iga yolg’on DNS-serverni kiritish mumkin.

Bu quyidagi algoritm bo’yicha amalga oshiriladi:

1. DNS-so’rovni kutish.

2. Olingan so’rovdan kerakli ma`lumotni chiqarib olish va tarmoq bo’yicha so’rov yuborgan xostga yolg’on DNS-javobni xaqiqiy DNS-server nomidan uzatish. Bu javobda yolg’on DNS-serverning IP-adresi ko’rsatilgan bo’ladi.

3. Xostdan paket olinganida paketning IP-sarlavxasidagi IP-adresni yolg’on DNS serverning IP-adresiga o’zgartirish va paketni serverga uzatish (ya`ni yolg’on DNS-server o’zining nomidan server bilan ish olib boradi).

4. Serverdan paketni olishda paketning IP-sarlavxasidagi IP-adresni yolg’on DNS-serverning IP-adresiga o’zgartirish va paketni xostga uzatish (yolg’on DNS serverni xost xaqiqiy xisoblaydi).

Yolg’on marshrutni kiritish. Ma`lumki, zamonaviy global tarmoqlari bir-biri bilan *tarmoq tugunlari* yordamida ulangan tarmoq segmentlarining majmuidir. Bunda *marshrut* deganda ma`lumotlarni manbadan qabul qiluvchiga uzatishga xizmat qiluvchi tarmoq tugunlarining ketma-ketligi tushuniladi. Marshrutlar xususidagi axborotni almashishni unifikatsiyalash uchun marshrutlarni boshqaruvchi maxsus protokollar mavjud. Internetdagi bunday protokollarga yangi marshrutlar xususida xabarlar almashish protokoli – ICMP (Internet Control Message Protocol) va marshrutizatorlarni masofadan boshqarish protokoli SNMP (Simple Network Manegment Protocol) misol bo’laoladi. Marshrutni o’zgartirish xujum qiluvchi yolg’on xostni kiritishdan bo’lak narsa emas. Xatto oxirgi ob yekt xaqiqiy bo’lsa, xam marshrutni axborot baribir yolg’on xostdan o’tadigan qilib qurish mumkin.

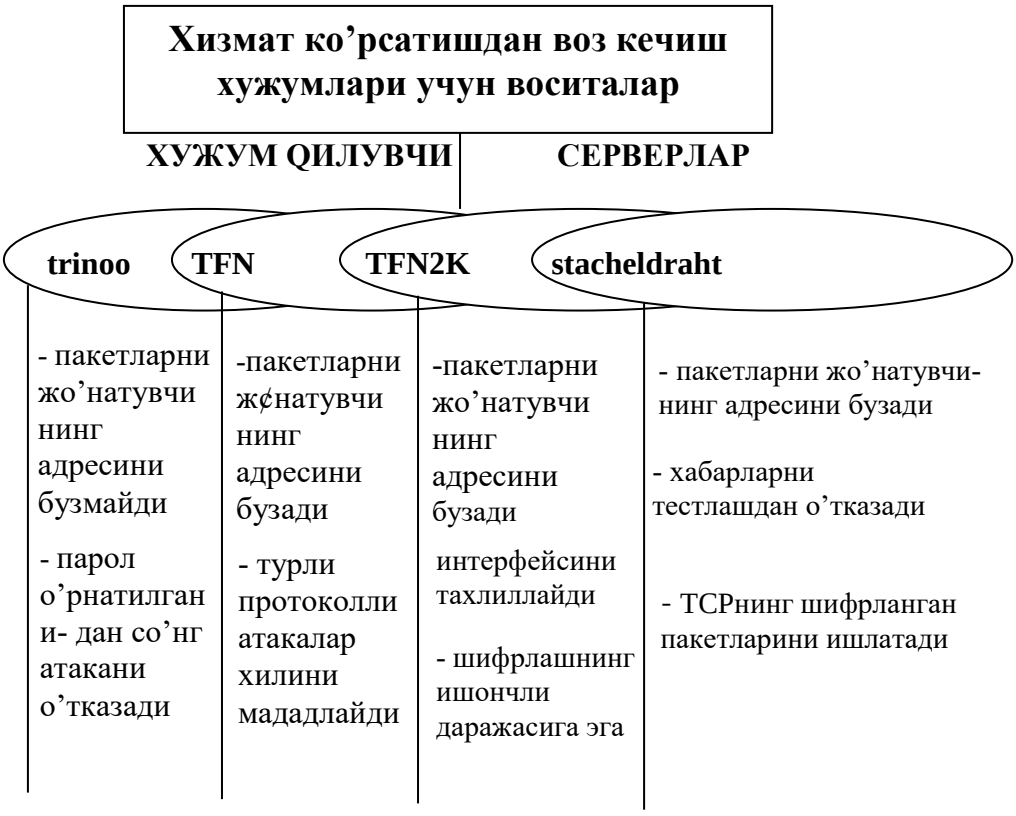
Marshrutni o’zgartirish uchun xujum qiluvchi tarmoqqa tarmoqni boshqaruvchi qurilmalar (masalan, marshrutizatorlar) nomidan berilgan tarmoqni boshqaruvchi protokollar orqali aniqlangan maxsus xizmatchi xabarlarni jo’natishi lozim. Marshrutni muvaffaqiyatli o’zgartirish natijasida xujum qiluvchi taqsimlangan tarmoqdagi ikkita ob yekt almashadigan axborot oqimidan to’la nazoratga ega bo’ladi, so’ngra axborotni ushlab qolishi, taxlillashi, modifikatsiyalashi yoki oddiygina yo’qotishi mumkin. Boshqacha aytganda taxdidlarning barcha turlarini amalga oshirish imkoniyati tug’iladi.

Xizmat qilishdan voz kechishga undaydigan taqsimlangan xujumlar – DdoS (Distributed Denial of Service) Kompyuter jinoyatchiligining nisbatan yangi xili bo’lsada, qo’rqinchli tezlik bilan tarqalmoqda. Bu xujumlarning o’zi anchagina yoqimsiz bo’lgani yetmaganidek, ular bir vaqtning o’zida masofadan boshqariluvchi yuzlab xujum qiluvchi serverlar tomonidan boshlanishi mumkin.

Xakerlar tomonidan tashkil etilgan tugunlarda DDoS xujumlar uchun uchta instrumental vositani topish mumkin: trinoo, Tribe FloodNet (TFN) va TFN2K. Yaqinda TFN va trinooning eng yoqimsiz sifatlarini uyg’unlashtirgan yana bittasi stacheldraht ("tikon simlar") paydo bo’ldi.

2.3-rasmda xizmat qilishdan voz kechishga undaydigan xujum vositalarining xarakteristikalari keltirilgan.

Xizmat qilishdan voz kechishga undaydigan oddiy tarmoq xujumida xaker tanlagan tizimiga paketlarni junatuvchi instrumentidan foydalanadi. Bu paketlar nishon tizimining to’lib toshishi va buzilishiga sabab bo’lishi kerak. Ko’pincha bunday paketlarni junatuvchilar adresi buzib ko’rsatiladi. Shu sababli xujumning xaqiqiy manbasini aniqlash juda qiyin.



2.3-расм. Хизмат килишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари

DDoS xujumlarini tashkil etish bitta xakerning qo'lidan keladi, ammo bunday xujumning effekti *agentlar* deb ataluvchi xujum qiluvchi serverlarning ishlatilishi xisobiga anchagina kuchayadi. TFNda *serverlar* (server), a trinooda *demonlar* (daemon) deb ataluvchi bu agentlar xaker tomonidan masofadan boshqariladi.

Axborot xavfsizligini buzuvchining modeli. Bo'lishi mumkin bo'lgan taxdidlarni oldini olish uchun nafaqat operatsion tizimlarni, dasturiy ta`minotni ximoyalash va foydalanishni nazorat qilish, balki buzuvchilar turkumini va ular foydalanadigan usullarni aniqlash lozim.

Sabablar, maqsadlar va usullarga bog'liq xolda axborot xavfsizligini buzuvchilarni to'rtta kategoriyaga ajratish mumkin:

- sarguzasht qidiruvchilar;
- g'oyaviy xakerlar;
- xakerlar-professionallar;
- ishonchsiz xodimlar.

Sarguzasht qidiruvchi, odatda, yosh, ko'pincha talaba yoki yuqori sinf o'quvchisi va unda o'ylab qilingan xujum rejasi kamdan-kam bo'ladi. U nishonini tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi. Xavfsizlik tizimida nuqsonli joyni topib, u maxfiy axborotni yig'ishga tirishadi, ammo xech qachon uni yashirincha o'zgartirishga urinmaydi. Bunday sarguzasht qidiruvchi muvaffaqiyatlarini fakat yaqin do'stlari–kasbdoshlari bilan o'rtoqlashadi.

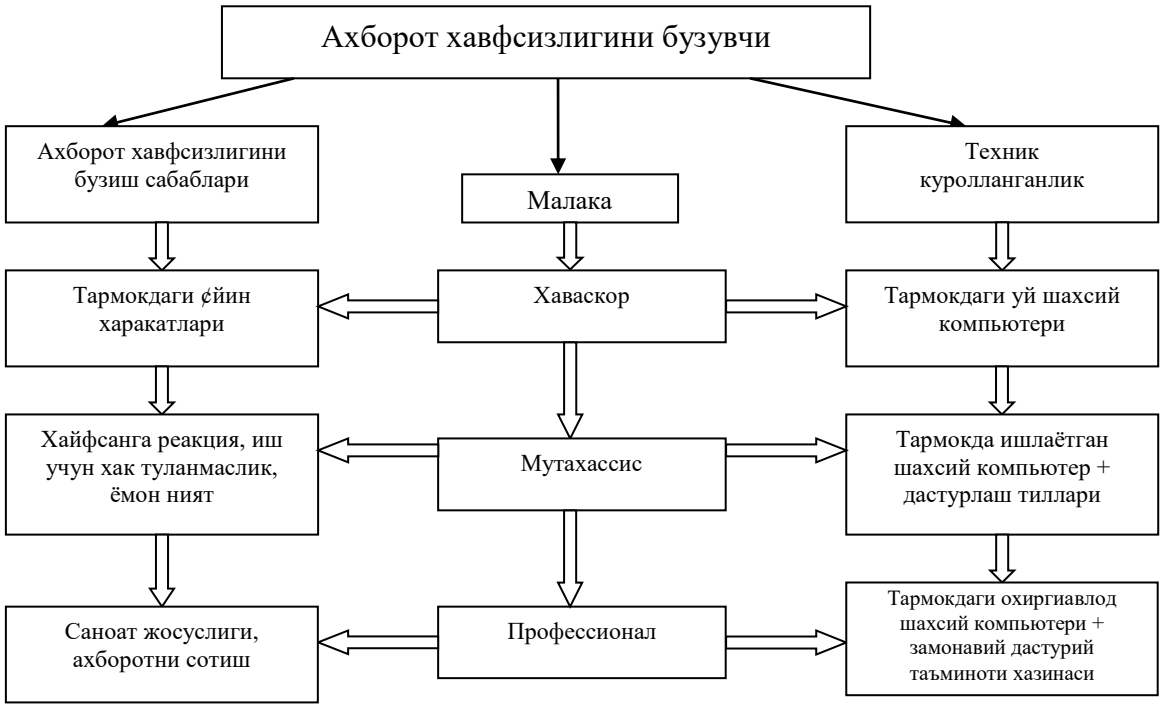
G'oyali xaker – bu xam sarguzasht qiduruvchi, ammo moxirroq. U o'zining e`tiqodi asosida muayyan nishonlarni (xostlar va resurslarni) tanlaydi. Uning yaxshi ko'rgan xujum turi Web-serverning axborotini o'zgartirishi yoki, juda kam xollarda, xujum qilinuvchi resurslar ishini blokirovka qilish. Sarguzasht qidiruvchilarga nisbatan g'oyali xakerlar muvaffaqiyatlarini kengrok auditoriyada, odatda axborotni xaker Web-tugunda yoki Usenet anjumanida joylashtirilgan xolda e`lon qiladilar.

Xaker-proffesional xarakatlarning aniq rejasiga ega va ma`lum resurslarni mo'ljallaydi. Uning xujumlari yaxshi o'ylangan va odatda bir necha bosqichda

amalga oshiriladi. Avval u dastlabki axborotni yig'adi (operatsion tizim turi, taqdim etiladigan servislar va qo'llaniladigan ximoya choralari). So'ngra u yig'ilgan ma`lumotlarni xisobga olgan xolda xujum rejasini tuzadi va mos instrumentlarni tanlaydi (yoki xatto ishlab chiqadi). Keyin, xujumni amalga oshirib, maxfiy axborotni oladi va nixoyat xarakatlarining barcha izlarini yo'q qiladi. Bunday xujum qiluvchi professional, odatda yaxshi moliyalanadi va yakka yoki professionallar komandasida ishlashi mumkin.

Ishonchsiz xodim o'zining xarakatlari bilan sanoat josusi yetkazadigan muammoga teng (undan xam ko'p bo'lishi mumkin) muammoni tug'diradi. Buning ustiga uning borligini aniqlash murakkabroq. Undan tashqari unga tarmoqning tashqi ximoyasini emas, balki faqat, odatda unchalik kat iy bo'lmagan tarmoqning ichki ximoyasini bartaraf qilishiga to'g'ri keladi. Ammo, bu xolda uning korporativ ma`lumotlardan ruxsatsiz foydalanishi xavfi boshqa xar qanday niyati buzuq odamnikidan yuqori bo'ladi.

Yuqorida keltirilgan axborot xavfsizligini buzuvchilar kategoriyalarini ularni malakalari bo'yicha guruxlash mumkin: xavaskor (sarguzasht qidiruvchi), mutaxassis (g'oyali xaker, ishonchsiz xodim), professional (xaker-professional). Agar bu guruxlar bilan xavfsizlikning buzilishi sabablari va xar bir guruxning texnik qurollanganligi taqqoslansa, axborot xavfsizligini buzuvchining umumlashtirilgan modelini olish mumkin (2.4-rasm).



2.4-расм. Ахборот хавфсизлигини бузувчининг модели

Axborot xavfsizligini buzuvchi, odatda ma`lum malakali mutaxassis bo'lgan xolda Kompyuter tizimlari va tarmoqlari xususan, ularni ximoyalash vositalari xususida barcha narsalarni bilishga urinadi. Shu sababli buzuvchi modeli quyidagilarni aniklaydi:

- buzuvchi bo'lishi mumkin bo'lgan shaxslar kategoriyasi;
- buzuvchining bo'lishi mumkin bo'lgan nishonlari va ularning muximlik va xavfsizlik darajasi bo'yicha rutbalanishi;
- uning malakasi xususidagi taxminlar; uning texnik qurollanganligining baxosi;
- uning xarakat xarakteri bo'yicha cheklashlar va taxminlar.

Tizimdan ruxsatsiz foydalanishga majbur etish sabablarining diapazoni yetarlicha keng: Kompyuter bilan o'ynaganidagi xayajon ko'tarinkiligidan to jirkanch menedjer ustidan xokimlik xissiyotigacha. Bu bilan nafaqat ko'ngil ochishni xoxlovchi xavaskorlar, balki professional dasturchilar ham shug'ullanadi. Ular parolni tanlash, faraz qilish natijasida yoki boshqa xakerlar bilan almashish yo'li orqali qo'lga kiritadilar. Ularning bir qismi nafaqat fayllarni ko'rib chiqadi,

balki fayllarning mazmuni bilan qiziqa boshlaydi. Bu jiddiy taxdid xisoblanadi, chunki bu xolda beozor shuxlikni yomon niyat bilan qilingan xarakatdan ajratish qiyin bo'ladi.

Yaqin vaqtgacha raxbarlardan norozi xizmatchilarning o'z mavqelarini suiiste`mol qilgan xolda tizimni buzishlari, undan begonalarning foydalanishlariga yo'l qo'yishlari yoki tizimni ish xolatida qarovsiz qoldirishlari tashvishlantirar edi. Bunday xarakatlarga majbur etish sabablari quyidagilar:

- xayfsanga yoki raxbar tomonidan tanbexga reaktsiya;
- ish vaqtidan tashqari bajarilgan ishga firma xaq to'lamaganidan norozilik;
- firmani qandaydir yangi tuzilayotgan firmaga raqib sifatida zaiflashtirish maqsadida qasos olish kabi yomon niyat.

Raxbardan norozi xodim jamoa foydalanuvchi xisoblash tizimlariga eng katta taxdidlardan birini tug'diradi. Shuning uchun xam xakerlar bilan kurashish agentligi individual Kompyuter soxiblariga jon deb xizmat ko'rsatadilar.

Professional xakerlar-xisoblash texnikasini va aloka tizimini juda yaxshi biladigan Kompyuter fanatlari (mutaassiblari) xisoblanadi. Tizimga kirish uchun professionallar omadga va farazga tayanmaydilar va qandaydir tartibni va tajribani ishlatadilar. Ularning maksadi- ximoyani aniqlash va yo'qotish, xisoblash kurilmasining imkoniyatlarini o'rganish va maqsadiga erishish mumkinligi to'g'risida qarorga kelish.

Bunday professional xakerlar kategoriyasiga quyidagi shaxslar kiradi:

- siyosiy maqsadni ko'zlovchi jinoiy guruxlarga kiruvchilar;
- sanoat josuslik maqsadlarida axborotni olishga urinuvchilar;
- tekin daromadga intiluvchi xakerlar guruxi.

Umuman professional xakerlar xavf-xatarni minimallashtirishga urinadilar. Buning uchun ular birga ishlashga firmada ishlaydigan yoki firmadan yaqinda ishdan bo'shatilgan xodimlarni jalb etadilar, chunki begona uchun bank tizimiga kirishda oshkor bo'lish xavfi juda katta. Xaqiqatan, bank xisoblash tizimlarining murakkabligi va yuqori tezkorligi, xujjatlarni yurgizish va tekshirish usullarining muntazam takomillashtirilishi begona shaxs uchun xabarlarni ushlab kolish yoki

ma`lumotlarni o’g’irlash maqsadida tizimga o’rnashishiga imkon bermaydi. Professional xakerlar uchun yana bir qo’shimcha xavotir-tizimdagi bir komponentning o’zgarishi boshqa bir komponentning buzilishiga olib kelishi va xatardan darak beruvchi signalga sabab bo’lishi mumkin.

Xakerlar xavf-xatarni kamaytirish maqsadida odatda moliyaviy va oilaviy muammolarga ega bo’lgan xodimlar bilan kontaktga kiradilar. Ko’pgina odamlar xayotida xakerlar bilan to’qnashmasliklari mumkin, ammo alkagolga yoki qimorga ruju qo’ygan xodimlar bilmasdan jinoiy gurux bilan bog’langan qandaydir bir bukmekerdan qarzdor bo’lib qolishlari mumkin. Bunday xodim qandaydir o’yin-kulgi kechasida suxbatdoshining professional agent ekanligiga shubxa qilmagan xolda ortiqcha gapirib yuborishi mumkin.

XULOSA

Ushbu bo’limda axborotxavfsizligiga taxdidlar to’g’risida ma`lumotlar keltirilgan. Bunda asosan, tizim va tarmoqlarda taxdidlar va zaifliklar, xavfsizlikning buzilish manbalari, axborot tizimid zaif joylarning paydo bo’lishi va joylashish klassifikatsiyasi, ruxsatsiz kirishning mumkin bo’lgan asosiy usullari, axborotga shtatli murojaat qilish vositalarining turlari keltirilgan.

Kompyuter qaroqchilari xakerlar, krakerlar to’g’risida ma`lumotlar keltirilgan.

Bundan tashqari tarmoqdagi axborotga bo’ladigan namunaviy xujumlar, tarmoqlar trafigini taxlillash, yolg’on ma`lumot yoki marshrutni kiritish, xizmat qilishdan voz kechishga undaydigan xujum vostalarining xarakteristikalari, maqsadlar va usullarga bog’liq xolda axborot xavfsizligini buzuvchilarni kategoriyalari va axborot xavfsizligini buzuvchining modeli keltirilgan.

3. MA`LUMOT UZATISh TARMOQLARIDA XAVFSIZLIK TAXDIDLARINI TAXLILI

3.1. Xavfsizlikni adaptiv boshqarish kontseptsiyasi

Tashkilotlarda ximoyalash bilan bog'liq bo'lgan muammolarni yechish uchun aksariyat xollarda qisman yondashishlardan foydalanishadi. Bu yondashishlar, odatda, avvalo foydalana oluvchi resurslarning joriy darajasi orqali aniqlanadi. Undan tashqari, xavfsizlik ma`murlari ko'pincha o'zlariga tushunarli bo'lgan xavfsizlik xavf-xatarlariga reaktsiya ko'rsatishadi. Aslida xavf-xatarlar juda ko'p bo'lishi mumkin. Korporativ axborot tizimini faqat qat`iy joriy nazorati va xavfsizlikning umumiy siyosatini ta`minlovchi kompleks yondashish xavfsizlik xavf-xatarlarini anchagina kamaytirishi mumkin.

Oxirgi vaqtda turli kompaniyalar tomonidan qator yondashishlar ishlab chiqildiki, bu yondashishlar nafaqat mavjud zaifliklarni aniqlashga, balki o'zgargan eski yoki paydo bo'lgan yangi zaifliklarni aniqlashga va ularga mos ximoyalash vositalarini qarshi qo'yishga imkon beradi. Xususan, ISS(Internet Security Systems) kompaniyasi tomonidan *xavfsizlikni adaptiv boshqarish modeli* ANS (Adaptive Network Security) ishlab chiqildi.

Xavfsizlikka adaptiv yondashish, to'g'ri loyixalangan va yaxshi boshqariluvchi jarayon va vositalar yordamida xavfsizlik xavf-xatarlarini real vaqt rejimida nazoratlash, aniqlash va ularga reaktsiya ko'rsatishga imkon beradi.

Tarmoqning adaptiv xavfsizligi quyidagi asosiy uchta element orqali ta`minlanadi:

- xavf-xatarlarni baxolash;
- ximoyalanishni taxlillash;
- xujumlarni aniqlash.

Xavf-xatarlarni baxolash. Xavf-xatarlarni (keltiradigan zararning jiddiylik darajasi bo'yicha), tarmoq qism tizimlarini (jiddiylik darajasi bo'yicha), taxdidlarni (ularning amalga oshirilishi extimolligi bo'yicha) aniqlash va rutbalashdan iborat.

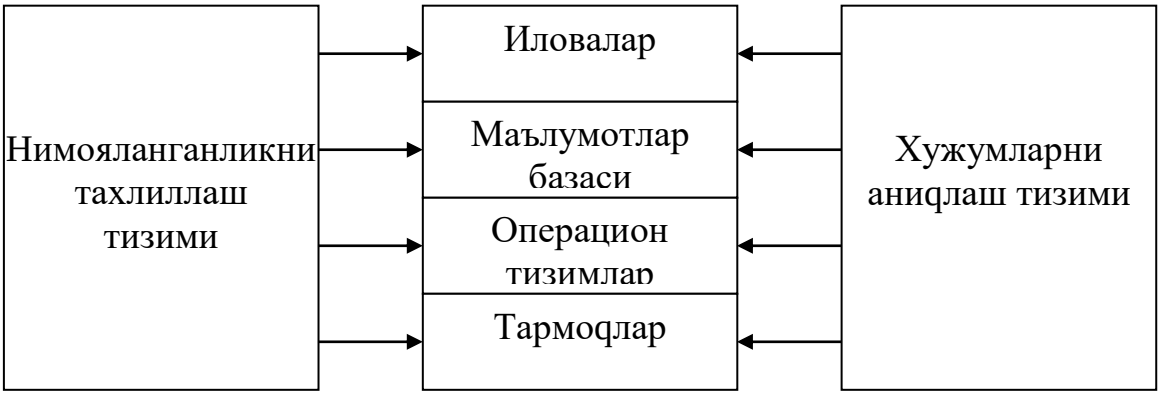
Tarmoq konfiguratsiyasi muttasil o’zgarishi sababli, xavf-xatarlarni baxolash jarayoni xam uzluksiz o’tkazilishi lozim. Korporativ axborot tizimining ximoyalash tizimini qurish xavf-xatarlarni baxolashdan boshlanishi lozim.

Ximoyalanishni taxlillash – tarmoqning zaif joylarini qidirish. Tarmoq ulanishlardan, tugunlardan, xostlardan, ishchi stantsiyalardan, ilovalardan va ma`lumot bazalaridan tarkib topgan. Bularning barchasi ximoyalanishlar samaradorligining xamda no`malum zaifliklarining aniqlanishiga muxtoj. Ximoyalanishni taxlillash texnologiyasi tarmoqni tadqiqlash, nozik joylarini topish, bu ma`lumotlarni umumlashtirish va ular bo’yicha xisobot berish imkoniyatiga ega. Agar bu texnologiyani amalga oshiruvchi tizim adaptiv komponentga xam ega bo’lsa, aniqlangan zaifliklarni avtomatik tarzda bartaraf etish mumkin. Ximoyalanishni taxlillash texnologiyasi tarmoq xavfsizligi siyosatini, uni tashkilot tashqarisidan yoki ichkarisidan buzishga urinishlardan oldin, amalga oshirishga imkon beruvchi ta`sirchan usul xisoblanadi.

Ximoyalanishni taxlillash texnologiyasi tomonidan identifikatsiyalanuvchi muammolarning ba`zilari quyidagilar:

- tizimlardagi "teshiklar" (back door) va troyan oti xilidagi dastur;
- kuchsiz parollar;
- ximoyalanmagan tizimdan suqilib kirishga va "xizmat qilishdan voz kechish" xilidagi xujumlarga ta`sirchanlik;
- operatsion tizimlardagi zaruriy yangilanishlarning yo’qligi;
- tarmoqlararo ekranlarning, Web-serverlarning va ma`lumotlar bazasining noto’g’ri sozlanishi va x.

Xujumlarni aniqlash – korporativ tarmoqdagi shubxali xarakatlarni baxolash jarayoni. Xujumlarni aniqlash operatsion tizim va ilovalarni qaydlash jurnallarini yoki real vaqtdagi trafikni taxlillash orqali amalga oshiriladi. Tarmoq tugunlari yoki segmentlarida joylashtirilgan xujumlarni aniqlash komponentlari turli xodisalarni, xususan, ma`lum zaifliklardan foydalanuvchi xarakatlarni xam baxolaydi (3.1-rasm).



3.1-расм. Нимояланганликни тахлиллаш ва хужумларни аниқлаш тизимларининг o’заро алоқаси

3.2–расм. Хавфсизликни бошқариш адаптив (мослашувчан) модели

Xavfsizlikni adaptiv boshqarish modeli ANSning adaptiv komponenti, yangi zaifliklar xususidagi eng oxirgi axborotni taqdim qilgan xolda, ximoyalanishni taxlillash jarayonini modifikatsiyalashga javob beradi. U xujumlarni aniqlash komponentini xam, uni xujumlar xususidagi oxirgi axborot bilan to’ldirish orqali, modifikatsiyalaydi. Adaptiv komponentning misoli sifatida yangi viruslarni aniqlash uchun virusga qarshi dasturning ma`lumotlar bazasini yangilash mexanizmini ko’rsatish mumkin.

Xavfsizlikni adaptiv boshqarish modelidan (3.2-rasm) foydalanish barcha taxdidlarni nazoratlash va ularga o’z vaqtida samarali reaktsiya ko’rsatish imkonini beradi. Bu esa o’z navbatida, nafaqat taxdidlarning amalga oshirilishiga sabab bo’luvchi zaifliklarni bartaraf qilishga, balki zaifliklar paydo bo’lish sharoitlarini taxlillashga imkon beradi.

3.2–расм. Хавфсизликни бошқариш адаптив (мослашувчан) модели

Tarmoq xavfsizligini adaptiv boshqarish modeli tarmoqda suiiste`mol qilishni kamaytirishga, tarmoqdagi xodisalardan foydalanuvchilar, ma`murlar va kompaniya raxbariyatining xabardorlik darajasini oshishiga xam imkon beradi. Ta`kidlash lozimki, ushbu model oldin ishlatiluvchi ximoyalash mexanizmlaridan (foydalanishni chegaralash, autentifikatsiyalash va x.) voz kechmaydi. Ularning funktsionalligini yangi texnologiya evaziga kengaytiradi. O'zlarining axborot xavfsizligini ta`minlash tizimlarini zamonaviy talablarga mos kelishini xoxlovchi tashkilotlar mavjud yechimlarni uchta yangi komponent-ximoyalanishni taxlillash, xujumlarni aniqlash va xavf-xatarni baxolash bilan to'ldirishi lozim.

3.2. Xujumlarni aniqlash

Tarmoq axborotini taxlillash usullari. Moxiyati bo'yicha, xujumlarni aniqlash jarayoni korporativ tarmoqda bo'layotgan shubxali xarakatlarni baxolash jarayonidir. Boshqacha aytganda xujumlarni aniqlash- xisoblash yoki tarmoq resurslariga yo'naltirilgan shubxali xarakatlarni identifikatsiyalash va ularga

reaktsiya ko’rsatish jarayoni. Xozirda xujumlarni aniqlash tizimida quyidagi usullar ishlatiladi:

- statistik usul;
- ekspert tizimlari;
- neyron tarmoqlari.

Statistik usul. Statistik yondashishning asosiy afzalligi – allaqachon ishlab chiqilgan va o’zini tanitgan matematik statistika apparatini ishlatish va sub`ekt xarakteriga moslash.

Avval taxlillanuvchi tizimning barcha sub`ektlari uchun profillar aniqlanadi. Ishlatiladigan profillarning etalondan xar qanday chetlanishi ruxsat etilmagan foydalanish xisoblanadi. Statistik usullar universal xisoblanadi, chunki mumkin bo’lgan xujumlarni va ular foydalanadigan zaifliklarni bilish talab etilmaydi. Ammo bu usullardan foydalanishda bir qancha muammolar paydo bo’ladi:

1. Statistik tizimlar xodisalar kelishi tartibiga sezuvchanmaslar; ba`zi xollarda bir xodisaning o’zi, kelishi tartibiga ko’ra anomal yoki normal faoliyatni xarakterlashi mumkin.

2. Anomal faoliyatni adekvat identifikatsiyalash maqsadida xujumlarni aniqlash tizimi tomonidan kuzatiluvchi xarakteristikalar uchun chegaraviy (bo’sag’aviy) qiymatlarni berish juda qiyin.

3. Statistik usullar vaqt o’tishi bilan buzg’unchilar tomonidan shunday "o’rnatilishi" mumkinki, xujum xarakatlari normal kabi qabul qilinadi.

Ekspert tizimlari. Ekspert tizimi odam-ekspert bilimlarini qamrab oluvchi qoidalar to’plamidan tashkil topgan. Ekspert tizimidan foydalanish xujumlarni aniqlashning keng tarqalgan usuli bo’lib, xujumlar xususidagi axborot qoidalar ko’rinishida ifodalanadi. Bu qoidalar xarakatlar ketma-ketligi yoki signaturalar ko’rinishida yozilishi mumkin. Bu qoidalarning xar birining bajarilishida ruxsatsiz faoliyat mavjudligi xususida qaror qabul qilinadi. Bunday yondashishning muxim afzalligi – yolg’on trevoganing umuman bo’lmasligi.

Ekspert tizimining ma`lumotlari bazasida xozirda ma`lum bo’lgan aksariyat xujumlar stsenariyasi bo’lishi lozim. Ekspert tizimlari, dolzarblikni saqlash

maqsadida, ma`lumotlar bazasini muttasil yangilashni talab etadi. Garchi ekspert tizimlari qaydlash jurnallaridagi ma`lumotlarni ko’zdan kechirishga yaxshi imkoniyatni tavsiya qilsada, so’ralgan yangilanish e`tiborsiz qoldirilishi yoki ma`mur tomonidan qo’lda amalga oshirilishi mumkin. Bu eng kamida, ekspert tizimi imkoniyatlarining bo’shashiga olib keladi.

Ekspert tizimlarining kamchiliklari ichida eng asosiysi – noma`lum xujumlarni akslantira olmasligi. Bunda oldindan ma`lum xujumning xatto ozgina o’zgarishi xujumlarni aniqlash tizimining ishlashiga jiddiy to’siq bo’lishi mumkin.

Neyron tarmoqlari. Xujumlarni aniqlash usullarining aksariyati qoidalar yoki statistik yondashish asosida nazoratlanuvchi muxitni taxlillash shakllaridan foydalanadi. Nazoratlanuvchi muxit sifatida qaydlash jurnallari yoki tarmoq trafigi ko’rilishi mumkin. Bunday taxlillash ma`mur yoki xujumlarni yaniqlash tizimi tomonidan yaratilgan, oldindan aniqlangan qoidalar to’plamiga tayanadi.

Xujumni vaqt bo’yicha yoki bir necha niyati buzuq odamlar o’rtasida xar qanday bo’linishi ekspert tizimlar yordamida aniqlashga qiyinchilik tug’diradi. Xujumlar va ular usullarining turli-tumanligi tufayli, ekspert tizimlari qoidalarining ma`lumotlar bazasining xatto doimiy yangilanishi ham xujumlar diapazonini aniq identifikatsiyalashni kafolatlamaydi.

Neyron tarmoqlaridan foydalanish ekspert tizimlarining yuqorida keltirilgan muammolarni bartaraf etishning bir usuli xisoblanadi. Ekspert tizimlari foydalanuvchiga ko’rilayotgan xarakteristikalar qoidalar ma`lumotlari bazasidagiga mos kelishi yoki mos kelmasligi xususida aniq javob beraolsa, neyrotarmoq axborotni taxlillaydi va ma`lumotlarni aniqlashga o’rgangan xarakteristikalariga mos kelishini baxolash imkoniyatini taqdim etadi. Neyrotarmoqli ifodalashning moslik darajasi 100%ga yetishi mumkin, ammo tanlash xaqiqiyligi tamoman qo’yilgan masala misollarini taxlillash sifatiga bog’liq.

Avval predmet soxasining oldindan tanlab olingan misolida neyrotarmoqni to’g’ri identifikatsiyalashga "o’rgatishadi". Neyrotarmoq reaktsiyasi taxlillanadi, qoniqarli natijalarga erishish maqsadida tizim sozlanadi. Neyrotarmoq xam vaqt

o’tishi bilan, predmet soxasi bilan bog’liq ma`lumotlarni taxlillashni o’tkazishiga qarab "tajriba orttiradi".

Neyrotarmoqlarning suiiste`mol qilinishni aniqlashdagi muxim afzalligi, ularning atayin qilinadigan xujumlar xarakteristikalarini "o’rganish" va tarmoqda oldin kuzatilganiga o’xshamagan elementlarni identifikatsiyalash qobiliyatidir.

Yuqorida tavsiflangan xujumlarni aniqlash usullarining xar biri afzalliklarga va kamchiliklarga ega. Shu sababli, xozirda tavsiflangan usullarning faqat bittasidan foydalanuvchi tizimni uchratish qiyin. Odatda, bu usullar birgalikda ishlatiladi.

Xujumlarni aniqlash tizimlarining turkumlanishi. Xujumlarni aniqlash tizimlari IDS(Intrusion Detection System)da ishlatiluvchi xujumlarni aniqlovchi mexanizmlar bir necha umumiy usullarga asoslangan. Ta`kidlash lozimki, bu usullar bir-birini inkor etmaydi. Aksariyat tizimlarda bir necha usullarning kombinatsiyasidan foydalaniladi.

Xujumlarni aniqlash tizimlari quyidagi alomatlari bo’yicha turkumlanishi mumkin:

- reaktsiya ko’rsatish usuli bo’yicha;
- xujumlarni fosh etish usuli bo’yicha;
- xujum xususidagi axborotni yig’ish usuli bo’yicha.

Reaktsiya ko’rsatish usuli bo’yicha passiv va aktiv IDSlar farqlanadi. Passiv IDS lar xujum faktlarini qaydlaydi, ma`lumotlarni jurnal fayliga yozadi va ogoxlantirishlar beradi. Aktiv IDSlar, masalan, tarmoqlararo ekranni qayta konfiguratsiyalash yoki marshrutizatordan foydalanish ruyxatini generatsiyalash bilan xujumga qarshi xarakat qilishga urinadi.

Xujumlarni fosh etish usuli bo’yicha IDSlarni quyidagi ikkita kategoriyaga ajratish qabul qilingan:

- anomal xatti-xarakatni aniqlash (anomaly-based);
- suiiste`molliklarni aniqlash (misuse detection yoki signature-based).

Anomal xatti-xarakatni aniqlash yo’li bilan xujumlarni aniqlash texnologiyasi quyidagi gipotezaga asoslangan. Foydalanuvchining anomal xatti-

xarakati (ya`ni xujumi yoki qandaydir g’arazli xarakati) – normal xatti-xarakatdan chetlashish. Anomal xatti-xarakatga misol tariqasida qisqa vaqt oralig’ida ulanishlarning katta sonini, markaziy protsessorning yuqori yuklanishini va x. ko’rsatish mumkin.

Agar foydalanuvchining normal xatti-xarakati profilini bir ma`noda tavsiflash mumkin bo’lganida, xar qanday undan chetlanishlarni anomal xatti-xarakat sifatida identifkatsiyalash mumkin bo’lar edi. Ammo, anomal xatti-xarakat xar doim xam xujum bo’lavermaydi. Masalan, tarmoq ma`muri tomonidan yuborilgan ko’p sonli so’rovlarni xujumlarni aniqlash tizimi "xizmat ko’rsatishdan voz kechish" xilidagi xujum sifatida identifikatsiyalashi mumkin.

Ushbu texnologiya asosidagi tizimdan foydalanilganda ikkita keskin xolat yuz berishi mumkin:

- xujum bo’lmagan anomal xatti-xarakatni aniqlash va uni xujumlar sinfiga kiritish;

- anomal xatti-xarakat ta`rifiga mos kelmaydigan xujumlarni o’tkazib yuborish. Bu xolat xujum bo’lmagan anomal xatti xarakatni xujumlar sinfiga kiritishga nisbatan xavfliroq xisoblanadi.

Bu kategoriya tizimlarini sozlashda va ekspluatatsiyasida ma`mur quyidagi qiyinchiliklarga duch keladi:

- foydalanuvchi profilini qurish sermexnat masala bo’lib, ma`murdan katta dastlabki ishlarni talab etadi.

- yuqorida keltirilgan ikkita keskin xarakatlardan birining paydo bo’lishi extimolligini pasaytirish uchun foydalanuvchi xatti-xarakatining chegaraviy qiymatlarini aniqlash zarur.

Anomal xatti-xarakatlarni aniqlash texnologiyasi xujumlarning yangi xilini aniqlashga mo’ljallangan. Uning kimchiligi - doimo "o’rganish" zaruriyati.

Suiiste`molliklarni aniqlash yo’li bilan xujumlarni aniqlash texnologiyasining moxiyati xujumlarni signatura ko’rinishida tavsiflash va ushbu signaturani nazoratlanuvchi makonda (tarmoq trafigida yoki qaydlash jurnalida) qidirishdan iborat. Xujum signaturasi sifatida anomal faoliyatni xarakterlovchi

xarakatlar shabloni yoki simvollar satri ishlatilishi mumkin. Bu signaturalar virusga qarshi tizimlarda ishlatiluvchi ma`lumotlar bazasiga o’xshash ma`lumotlar bazasida saqlanadi. Ta`kidlash lozimki, virusga qarshi rezident monitorlar xujumlarni aniqlash tizimlarining xususiy xoli xisoblanadi. Ammo bu yo’nalishlar boshidan parallel rivojlanganlari sababli, ularni ajratish qabul qilingan. Ushbu xil tizimlar barcha ma`lum xujumlarni aniqlasada, yangi, xali ma`lum bo’lmagan xujumlarni aniqlay olmaydi.

Bu tizimlarni ekspluatatsiyasida xam ma`murlarga muammolarni duch keladi. Birinchi muammo - signaturalarni tavsiflash mexanizmlarini, ya`ni xujumlarni tavsiflovchi tillarni yaratish. Ikkinchi muammo, birinchi muammo bilan bog’liq bo’lib, xujumlarni shunday tavsiflash lozimki, uning barcha modifikatsiyalarini qaydlash imkoni tug’ilsin.

Xujum xususidagi axborotni yig’ish usuli bo’yicha turkumlash eng ommaviy xisoblanadi:

- tarmoq satxida xujumlarni aniqlash (network-based);
- xost satxida xujumlarni aniqlash (host-based);
- ilova satxida xujumlarni aniqlash (application-based).

Tarmoq satxida xujumlarni aniqlash tizimida tarmoqdagi trafikni eshitish orqali niyati buzuq odamlarning mumkin bo’lgan xarakatlari aniqlanadi. Xujumni qidirish "xostdan-xostgacha" printsipi bo’yicha amalga oshiriladi. Ushbu xilga taalluqli tizimlar, odatda xujumlar signaturasidan va "bir zumda" taxlillashdan foydalanib, tarmoq trafigini taxlillaydi. "Bir zumda" taxlillash usuliga binoan tarmoq trafigi real yoki unga yaqinroq vaqtda monitoringlanadi va mos aniqlash algoritmlaridan foydalaniladi. Ko’pincha ruxsatsiz foydalanish faoliyatini xarakterlovchi trafikdagi ma`lum satrlarni qidirish mexanizmlaridan foydalaniladi.

Xost satxida xujumlarni aniqlash tizimi ma`lum xostda niyati buzuq odamlarni monitoringlash, detektirlash va xarakatlariga reaktsiya ko’rsatishga atalgan. Tizim ximoyalangan xostda joylashib, unga qarshi yo’naltirilgan xarakatlarni tekshiradi va oshkor qiladi. Bu tizimlar operatsion tizim yoki

ilovalarning qaydlash jurnallarini taxlillaydi. Qaydlash jurnallarini taxlillash usulini amalga oshirish oson bo’lsada, u quyidagi kamchiliklarga ega:

- jurnalda qayd etiluvchi ma`lumotlar xajmining kattaligi nazoratlanuvchi tizim ishlashi tezligiga salbiy ta`sir ko’rsatadi;

- qaydlash jurnalini taxlillashni mutaxassislar yordamisiz amalga oshirib bo’lmaydi;

- xozirgacha jurnallarni saqlashning unifikatsiyalangan formati mavjud emas;

- qaydlash jurnallaridagi yozuvni taxlillash real vaqtda amalga oshirilmaydi.

IDSning uchinchi xili ma`lum ilovadagi muammolarni qidirishga asoslangan.

Xujumlarni aniqlash tizimining komponentlari va arxitekturasi. Mavjud yechimlarning taxlili xujumlarni aniqlashning namunaviy tizimi komponentlarining ro’yxatini keltirishga imkon beradi.

Kuzatish moduli nazoratlanuvchi makondan (qaydlash jurnali yoki tarmoq trafigi) ma`lumotlarni yig’ishni ta`minlaydi. Uning quyidagi nomlari xam uchraydi: sensor (sensor), monitor (monitor), zond(probe) va x. Xujumlarni aniqlash tizimi arxitekturasining qurilishiga bog’liq xolda kuzatish moduli boshqa komponentlardan aloxida, boshqa Kompyuterda joylashishi mumkin.

Xujumlarni aniqlash qism tizimi asosiy modul bo’lib, kuzatish modulidan olinadigan axborotni taxlillaydi. Ushbu taxlillash natijasi bo’yicha qism tizim xujumlarni identifikatsiyalash, reaktsiya ko’rsatish variantlari bo’yicha to’xtamga kelishi, ma`lumotlar omborida xujumlar xususidagi axborotni saqlashi mumkin va x.

Bilimlar bazasida, xujumlarni aniqlash tizimlarida ishlatiladigan usullarga bog’liq xolda, foydalanuvchilar va xisoblash tizim profillari, ruxsatsiz foydalanishlarni xarakterlovchi xujum signaturalari yoki shubxali satrlar saqlanishi mumkin. Bilimlar bazasi xujumlarni aniqlash tizimlarini ishlab chiqaruvchilari, tizimdan foydalanuvchilar yoki uchinchi tomon, masalan bu tizimni madadlovchi autsorsing kompaniyasi tomonidan to’ldirilishi mumkin.

*Ma`lumotlar ombori* xujumlarni aniqlash tizimi ishlashi jarayonida yig'ilgan ma`lumotlarning saqlanishini ta`minlaydi.

Grafik interfeys tizimning nixoyatda zaruriy komponenti bo'lib, xujumlarni aniqlash tizimi ishlashini boshqaruvchi operatsion tizimga bog'liq xolda de-fakto Windows va Unix standartlariga mos kelishi lozim.

Reaktsiya ko'rsatish qism tizimi aniqlangan xujumlar va boshqa nazoratlanuvchi xodisalarga reaktsiya ko'rsatishni amalga oshiradi. Mavjud tizimlarda ishlatiladigan reaktsiya ko'rsatish usullarini quyidagi uchta kategoriyaga ajratish mumkin:

- bildirish;
- saqlash;
- faol reaktsiya ko'rsatish.

Bildirish usuli bo'yicha xujum xususidagi axborot xavfsizlik ma`muriga tizimning konsoliga yoki elektron pochta bo'yicha, peydjerga faks yoki telefon orqali jo'natilishi mumkin.

Saqlash usuliga reaktsiya ko'rsatishning quyidagi variantlari taalluqli:

- xodisalarni ma`lumotlar bazasida qaydlash;
- xujumlarni real vaqt masshtabida tiklash.

Birinchi variant ximoyalashning boshqa tizimlarida xam keng qo'llaniladi. Ikkinchi variantni amalga oshirish uchun xujum qiluvchini kompaniya tarmog'iga o'tkazib yuborish va uning barcha xarakatlarini qaydlash lozim. Bu xavfsizlik ma`muriga keyin vaqtning real masshtabida (yoki berilgan tezlikda) xujum qiluvchi tomonidan qilingan barcha xarakatlarni tiklashga, muvaffaqiyatli taxlillashga va ularni keyinchalik bartaraf etishga xamda muxokama qilish jarayonida yig'ilgan axborotdan foydalanishga imkon beradi.

Faol reaktsiya ko'rsatish kategoriyasiga quyidagi variantlar taalluqli:

- xujum qiluvchi ishini blokirovka qilish;
- xujum qilunuvchi tugun bilan seansni tugallash;
- tarmoq asbob-uskunalari va ximoya vositalarini boshqarish.

Reaktsiya ko’rsatish mexanizmlarining ushbu kategoriyasi bir tomondan yetarlicha samarali bo’lsa, ikkinchi tomondan ulardan juda extiyotlik bilan foydalanish zarur, chunki ularni noto’g’ri ishlatish butun korporativ axborot tizimi ishga layoqatligining buzilishiga olib kelishi mumkin.

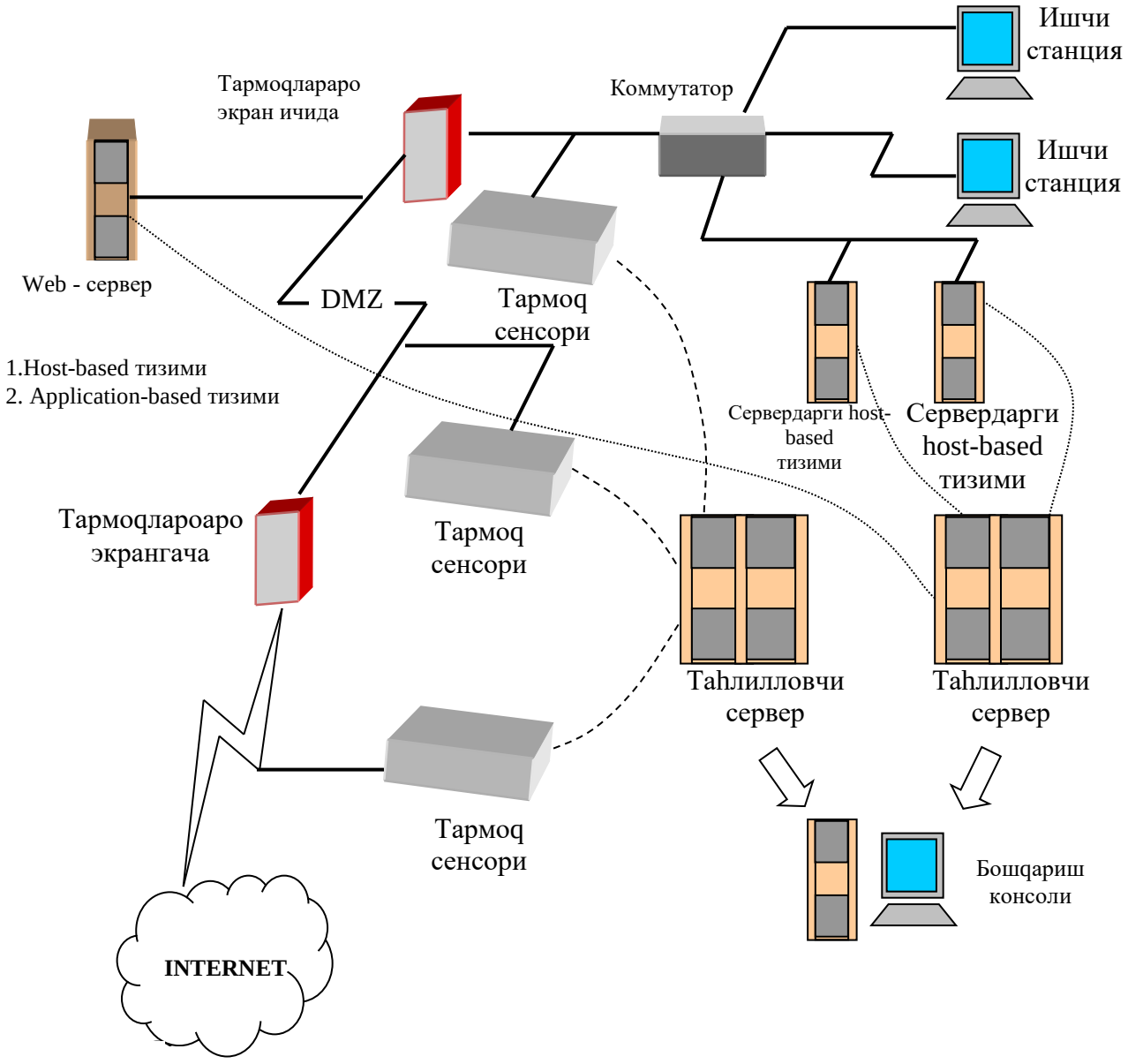
Komponentlarni boshqarish qism tizimi xujumlarni aniqlash tizimining turli komponentlarini boshqarishga atalgan. "Boshqarish" atamasi orqali xujumlarni aniqlash tizimining turli komponentlari (masalan kuzatish modullari) uchun xavfsizlik siyosatini o’zgartirish, xamda ushbu komponentlardan axborotni (masalan, qaydlangan xujum xususidagi) olish tushuniladi. Boshqarish ichki protokollar va interfeyslar va ishlab chiqilgan standartlar (masalan, SNMP) yordamida amalga oshirilishi mumkin.

Xujumlarni aniqlash tizimlari ikkita arxitektura – "avtonom agent" va "agent-menedjer" arxitekturalari asosida quriladi. Birinchi xolda tarmoqning xar bir ximoyalanuvchi tugun va segmentlariga tizim agentlari o’rnatilib, bu agentlar o’zaro axborot almasha olmaydilar, xamda ularni yagona konsol orqali markazlashtirilgan xolda boshqarib bo’lmaydi. "Agent-menedjer" arxitekturasi bu kamchiliklardan xoli. Bu xolda katta tarmoqning turli qismlarida joylashgan ko’pgina IDSdan iborat xujumlarni aniqlashning taqsimlangan tizimi dIDS (distributed IDS)da ma`lumotlarni yig’ish serverlari va markaziy taxlillovchi server qaydlanuvchi ma`lumotlarni markazlashtirilgan yig’ishni va taxlillashni amalga oshiradi. dIDS modullarini boshqarish boshqarishning markaziy konsoli orqali amalga oshiradi. Filiallari turli xududlar, xatto shaxarlar bo’yicha tarqalgan yirik tashkilotlar uchun bunday arxitekturaning ishlatilishi jiddiy axamiyatga ega.

dIDS ishlashining umumiy sxemasi 3.2-rasmda keltirilgan.

Bunday tizim turli IDSlardan xujumlar xususidagi axborotlarni markazlashtirilishi evaziga korporativ qism tarmoq ximoyalanishini kuchaytirishga imkon beradi. Xujumlarni aniqlovchi taqsimlangan tizim dIDS quyidagi qism tizimlardan tashkil topgan: boshqarish konsoli, taxlillovchi serverlar, tarmoq agentlari, xujum xususidagi axborotni yig’uvchi server. Markaziy taxlillovchi server odatda ma`lumotlar bazasi va Web-serverdan tashkil topgan bo’lib,

xujumlar xususidagi axborotni saqlashga va qulay Web-interfeys yordamida ma`lumotlarni manipulyatsiyalashga imkon beradi. Tarmoq agenti dIDSning eng muxim komponentlaridan biri xisoblanib, maqsadi markaziy taxlillovchi serverga xujum xususida xabar berish bo'lgan kichkina dasturdir. Xujum xususidagi axborotni yig'uvchi server markaziy taxlillovchi serverga mantiqiy tayangan va tarmoq agentlaridan olingan ma`lumotlarni guruxlashda foydalaniladigan parametrlarni belgilaydi.



3.2-расм. Таqсимланган IDS ишлашининг умумий схемаси

Ma`lumotlarni guruxlashni quyidagi parametrlar bo’yicha amalga oshirish mumkin:

- xujum qiluvchining IP-adresi;
- qabul qiluvchining porti;
- agent nomeri;
- sana, vaqt;
- protokol;
- xujum xillari va x.

IDSdan foydalanish samaradorligiga qandaydir shubxalar bo’lishiga qaramay, foydalanuvchilar IDSning ochiq tarqatiluvchi va tijorat vositalaridan keng foydalanadilar.

3.3. Ximoyalanishni taxlillash

Ximoyalanishni taxlillash vositalari zaifliklarni topib va o’z vaqtida yo’q qilib xujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, ximoyalash vositalarini ishlatilishiga bo’ladigan barcha sarf-xarajatlar kamayadi.

Ximoyalanishni taxlillash vositalari tarmoq satxida, operatsion tizim satxida va ilovalar satxida ishlashi mumkin. Ular tekshirishlar sonini bora-bora ko’paytirish, axborot tizimiga "ichkarilab borish" va uning barcha satxlarini tadqiqlash orqali zaifliklarni qidirishi mumkin.

Tarmoq protokollari va servislari ximoyalanishini taxlillash vositalari. Xar qanday tarmoqda abonentlarning o’zaro aloqasi ikkita va undan ko’p tugunlar orasida axborot almashinish muolajalarini belgilovchi tarmoq protokollari va servislaridan foydalanishga asoslangan. Tarmoq protokollari va servislarini ishlab chiqishda ularga ishlanuvchi axborot xavfsizligini ta`minlash bo’yicha talablar (odatda shubxasiz yetarli bo’lmagan) qo’yilgan. Shu sababli, tarmoq protokollarida aniqlangan zaifliklar xususida axborotlar paydo bo’lmoqda. Natijada, korporativ

tarmoqda foydalanadigan barcha protokol va servislarni doimo tekshirish zaruriyati tug’iladi.

Ximoyalanishni taxlillash tizimi zaifliklarni aniqlash bo’yicha testlar seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativ tarmoqlarga xujumlarida qo’llaniladiganiga o’xshash.

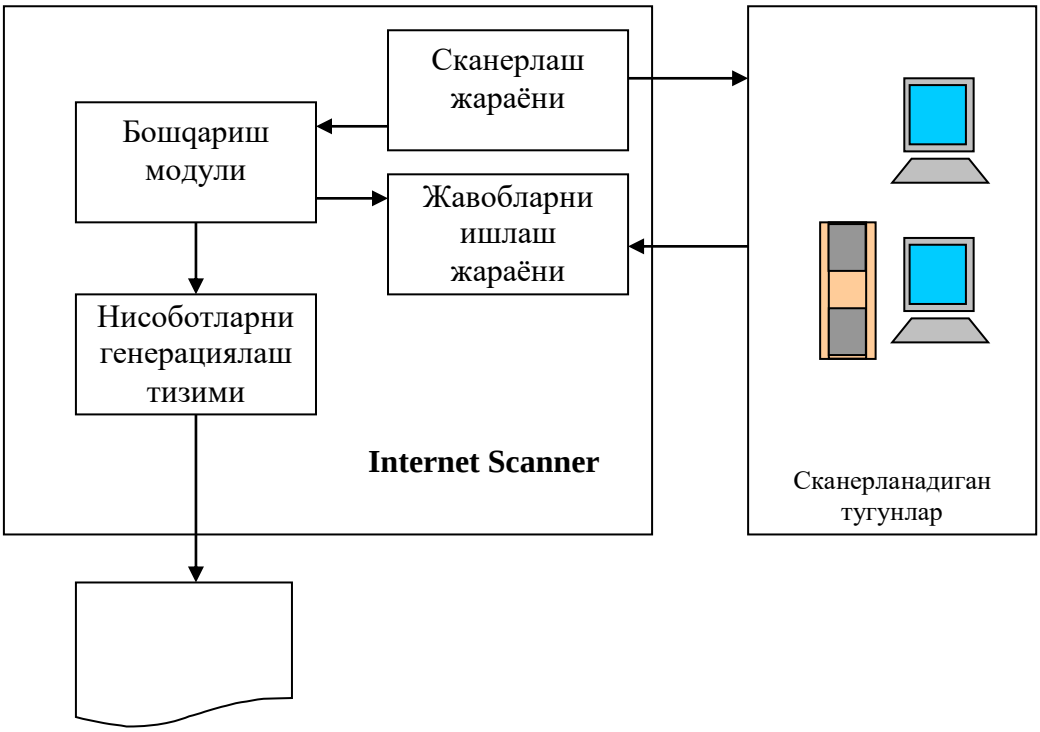
Zaifliklarni aniqlash maqsadida skanerlash tekshiruvchi tizim xususidagi dastlabki axborotni, xususan, ruxsat etilgan protokollar va ochiq portlar, operatsion tizimnnig ishlatiluvchi versiyalari va x. xususidagi axborotni olish bilan boshlanadi. Skanerlash keng tarqalgan xujumlar, masalan, to’liq saralash usuli bo’yicha parollarni tanlashdan foydalanib, suqilib kirishni imitatsiyalashga urinish bilan tugaydi.

Ximoyalanishni taxlillash vositalari yordamida tarmoq satxida nafaqat Internetning korporativ tarmoqdan ruxsatsiz foydalanishi imkoniyatini testlash, balki tashkilot ichki tarmog’ida tekshirishni amalga oshirish mumkin. Tarmoq satxida ximoyalanishni taxlillash tizimi tashkilot xavfsizlik darajasini baxolashga xamda tarmoq dasturiy va apparat ta`minotini sozlash samaradorligini nazoratlashga xizmat qiladi.

Ximoyalanishni taxlillashni amalga oshiruvchi (Internet Scanner tizimi misolida) namunaviy sxema 3.3-rasmda keltirilgan.

Ximoyalanishni taxlillash vositalarining bu sinfi nafaqat tarmoq protokollari va servislari, balki tarmoq bilan ishlashga javobgar tizimli va tatbiqiy dasturiy ta`minoti zaifiklarini xam taxlillaydi. Bunday ta`minot qatoriga Web, FTP, va pochta serverlarini, tarmoqlararo ekranlarni, brauzerlarni va x. kiritish mumkin.

Ba`zi vositalar dasturiy ta`minotni taxlillash bilan bir qatorda apparat vositalarini skanerlaydi. Bunday vositalarga kommutatsiyalovchi va marshrutlovchi asbob - uskunalar kiradi.



3.3–расм. Internet Scanner тизими мисолида ҳимояланганликни таҳлиллаш схемаси.

Operatsion tizim ximoyalanishini taxlillash vositalari. Vositalarning bu sinfi operatsion tizim ximoyalanishiga ta`sir etuvchi uning sozlanishlarini tekshirishga atalgan. Bunday sozlashlar quyidagilarni aniqlaydi:

- foydalanuvchilarning xisob yozuvi, masalan, parol uzunligi va uning ta`sir muddati;

- foydalanuvchilarning jiddiy tizimli fayllardan foydalanish xuquqlari;

- zaif tizimli fayllar;

- o’rnatilgan patchlar va x.

Operatsion tizim satxidagi ximoyalanishni taxlillash tizimlari operatsion tizimlar konfiguratsiyasini nazoratlashda xam ishlatilishi mumkin.

Tarmoq satxi ximoyalanishni taxlillash vositalaridan farqli ravishda, ushbu tizimlar taxlillanuvchi tizimni tashqaridan emas, balki ichkaridan skanerlaydi, ya`ni ular tashqaridagi niyati buzuq odamlar xujumlarini imitatsiyalamaydi. Operatsion tizim satxida ximoyalanishni taxlillash tizimlarining ba`zilari (masalan, Internet Security Systems kompaniyasining System Scanner tizimi) zaifliklarni aniqlash imkoniyatidan tashqari, aniqlangan muammolarning bir qismini avtomatik

tarzda bartaraf qilishga yoki tashkilotda qabul qilingan xavfsizlik siyosatini qoniqtirmaydigan tizim parametrlariga tuzatish kiritishga imkon beradi.

Tanlanuvchi ximoyalashni taxlillash vositalariga quyiladigan umumiy talablar. Tanlanuvchi tizimga qo'yiladigan majburiy talab-korxona tarmoq infratuzilmasini o'zgartirish zaruriyatining yo'qligi. Aks xolda bunday qaytadan tashkil etishga qilinadigan xarajat ximoyalanishni taxlillash tizimi narxidan oshib ketishi mumkin. Xozirda bu talabga faqat Internet Security Systems kompaniyasining Security Systems tizimi javob beradi.

Ximoyalanishni taxlillash vositalarini noto'g'ri ishlatish ulardan niyati buzuq odamlarning korporativ tarmoqqa suqilib kirish uchun foydalanishlariga imkon yaratadi. Shu sababli, ximoyalanishni taxlillash vositalari o'zlarining komponentlaridan va yig'ilgan ma`lumotlardan foydalanishni chegaralovchi mexanizmlar bilan ta`minlanishi lozim. Bunday mexanizmlarga quyidagilar kiradi:

- faqat ma`mur xuquqiga ega bo'lgan foydalanuvchi tomonidan ushbu vositalarni ishga tushirish;

- skanerlash ma`lumotlari arxivini shifrlash;

- masofadan boshqarishda ulanishni autentifikatsiyalash;

- kataloglar bilan ishlash uchun maxsus xuquqlarni aniqlash va x.

Zaifliklarni aniqlash jarayonining quyidagi imkoniyatlariga e`tiborni qaratish lozim:

- bir necha qurilma yoki servislarni parallel ishlash evaziga skanerlash tezligini oshirish;

- tizimdan ruxsatsiz foydalanishni oldini olish uchun xar bir skanerlanuvchi tugunga bildirish qog'ozini yuborish;

- yolg'on ishlashlarni minimallashtirish uchun tarmoqni ekspluatatsiya talablariga to'g'rilash.

Korporativ tarmoq xolatining doimo o'zgarib turishi, uning ximoyalanishiga ta`sir ko'rsatadi. Shu sababli, ximoyalanishni taxlillashning yaxshi tizimi jadval bo'yicha ishlash rejimiga ega bo'lib, ma`mur uni eslagunicha o'zi tarmoq tugunlari zaifliklarini tekshirishi va paydo bo'lgan muammolar xususida nafaqat ma`murni

ogoxlantirishi, balki aniqlangan zaifliklarni yo’qotish usullarini tavsiya etishi lozim.

E`tibor berish zarur bo’lgan xarakteristikalardan biri-xisobotlarni generatsiyalash tizimining mavjudligi. Bu tizim foydalanuvchilarning turli kategoriyalarlari – texnik mutaxassislardan tortib to tashkilotlar raxbarlari uchun tafsiloti turli darajada bo’lgan xujjatlarni yaratishga imkon berishi lozim.

Xujjatlarda ma`lumotlarni ifodalash shakli xam muxim xisoblanadi. Faqat matnli axborot bilan to’ldirilgan xujjatlarning foydasi bo’lmaydi. Grafiklardan foydalanish esa ma`murga tashkilot tarmog’idagi barcha muammolarni yaqqol namoyish etishga imkon beradi. Xisobotlarda aniqlangan muammolarni yo’qotish bo’yicha tavsiyalarning mavjudligi ximoyalanishni taxlillash vositalarini tanlashdagi majburiy shart xisoblanadi.

Doimo yangi zaifliklarning aniqlanishi ximoyalanishni taxlillash tizimining zaifliklar ma`lumotlari bazasini to’ldira olishi imkoniyatiga ega bo’lishini taqozo etadi. Bu zaifliklarni tavsiflovchi maxsus til yordamida yoki tizim ishlab chiqaruvchilari tomonidan zaifliklarni vaqti-vaqti bilan to’ldirish yo’li bilan amalga oshiriladi. Korporativ tarmoq tugunlarining ximoyalanish darajasining o’zgarishini taxlillash uchun tanlanuvchi vosita o’tkazilgan skanerlash seanslari xususidagi axborotni to’planishiga imkon berishi lozim.

XULOSA

Uchinchi bo’limda ma`lumot uzatish tarmoqlarida xavfsizlik taxdidlarini taxlili ko’rib chiqilgan. Bunda asosan tarmoqning adaptiv xavfsizligi turlari, xujumlarni aniqlash xavf-xatarlarni baxolash, ximoyalanganlikni taxlillash va xujumlarni aniqlash tizimlarining o’zaro aloqaslari, xavfsizlikni boshqarish adaptiv modellari to’g’risida ma`lumotlar keltirilgan.

Xujumlarni aniqlash usullar va ta`riflari, xujumlarni aniqlash tizimlarining turkumlanishi, komponentlari va arxitekturasi keltirilgan.

Ximoyalanishni taxlillash vositalari zaifliklarni topib, o’z vaqtida yo’q qilib xujumni amalga oshirishini bartaraf qiladi. Taxlil sifatida tarmoq protokollari va servislari ximoyalanishini taxlillashdan iborat. Ximoyalanishni taxlillash tizimi zaifliklarni aniqlash bo’yicha testlar seriyasini bajaradi.

4. XAYOT FAOLIYATI XAVFSIZLIGI

4.1. Operator ishlash joyidagi ergonomik talablar

Kiritish - chiqarish qurilmalarini (monitor klaviatura va sichqoncha) ergonomik ekspluatatsiya va sog'liqni asrash uchun mo'ljallangan. Shunindek, kiritish - chiqarish qurilmalarini nosoz ishlashi, qo'lni noto'g'ri yoki sichqoncha orqali axborot kiritish inson tanasining zo'riqishiga, mushaklarda nerv tizimini susayishiga, bo'g'imlarda og'riq paydo bo'lishiga xam sababchi bo'ladi. Bu xolat quyidagi maslaxatlarga amal qilinganda sezirarli darajada kamayishi mumkin.

Ish joyida monitor shunday joylanishi kerakki, yoruglik iloji boricha yuqoridan burchak ostida tushishi kerak. Monitor derazaga nisbatan turishi ish stoli esa yorituvchi qurilmalar orasida turishi kerak. Ko'zni zo'riqtiradigan to'g'ri (ko'rish maydoniga tushayotgan yorug'lik manbai) va qaytgan (ekrandan qaytgan yorug'lik) yorug'likdan iloji boricha ximoyalanish kerak. Buning uchun ish joyini o'zgartirishi kerak. Monitordagi tasvirning yoritilishini, ravshanligi va kontrasti bajarayotgan ishga va xonaning yoritilganligiga bog'liq xolda sozlanishi kerak.

Monitor, xujjatlar va klaviatura shunday joylashishi kerakki, ularni yorug'lik manbasiga nisbatan joylashganligiga bog'liq bo'lgan yuzalardagi ravshanlik 1:10 nisbatdan oshib ketmasligi kerak (1:3 nisbat tavsiya etiladi).

Klaviatura va sichqonchani shunday joylashtirish zarurki, ularning ekspluatatsiyasida sezilarli kuchlanishlar paydo bo'lmasligi kerak. Klaviaturani tananing yuqori qismiga nisbatan parallel ravishda, sichqonchani esa, aynan klaviatura orasi 5-10 sm bo'lishi kerak.

Monitorni shunday joylashtirish kerakki, undagi tasvirni boshni yoki tanani burmasdan ko'rish mumkin bo'lsin. Monitorgacha bo'lgan masofa 70 smdan oshmasligi zarur (optimal masofa 50 sm) xujjatlashtirish qurilmalari va tez-tez ishlatib turilmaydigan texnik vositalar operatordan o'ng tomonda, maksimal erishish zonasida joylashtirish aloqa vositalari esa chap tomonda o'ng qo'lni

yozish uchun bo’sh qoldirish maqsadida joylashtirish tavsiya etiladi. Xujjatgacha bo’lgan masofa xuddi monitor uchun mo’ljallangan masofadek bo’lishi kerak.

Stol yoki stulning balandligi operatorning bo’yiga qarab moslashtiriladi. Stulning suyanchigi umurtqa pog’onasini bel qismiga tegib turadigan va operator to’g’ri o’tira oladigan bo’lishi kerak.

Monitor tasvirning yuqori chekkasi ko’z chizig’ida bo’lishi zarur.

Bu maslaxatlarning xammasi PK bilan ishlashda tana a`zolarini toliqtirmasdan, zo’riqtirmasdan ishlashini ta`minlaydi.

4.2. Kompyuter texnikasi – nurlanish manbai va undan ximoyalanish

Ma`lumki, komp`yuter texnikasi elektromagnit nurlanish manbai xisoblanadi. U inson xayoti uchun xavfli, ayniqsa uni noto’g’ri ishlatganda bu masala O’zbekiston uchun o’ziga xos axamiyatli o’ringa ega. Chunki O’zbekistonda komp`yuter axborotlashtirish texnologiyalarini rivojlantirish bo’yicha katta ijobiy o’zgarishlar qilinmoqda.

Komp`yuter texnikasini ishlab chiqarish jarayonida avtomatikani, tezkorlikni, aniqlikni oshiradi. Lekin bu qurilmani ximoyasiz ishlatish inson salomatligiga salbiy ta`sir ko’rsatishi muqarrardir.

O’zbekistonda xam komp`ter texnikasini rivojlantirish bosqichlarida ularning soni ko’paytirildi. Bojxonadan o’tkazilayotgan komp`yuter texnikalarini ekologik me`yorlarga javob berishiga qaralmadi (chet ellarda elektro magnit xavfsizlik bo’yicha “Shved standarti” MPR II jaxon xamjamiyatida tan olingan). PK monitorlari uchun ekran fil trlari sifatini tartibga soluvchi biror bir xujjatlar yo’q. Natijada, bozor “absolyut”, ”to’liq”, “global” ximoya filtrlari reklamasi ko’payib ketdi. Tekshiruvlar natijasi esa, ularning ayrimlari chiroyli romchaga solingan oddiy shisha bo’lib chiqmoqda, lekin muammo faqat shunda emas, kom pyuter texnikasi bilan jixozlangan ish joylarida o’rnatilgan sarf darajasi gigienik me`yorlarga mos kelmayapti.

Ish joyida elektromagnit xavfsizlik muammosini xal qilish uchun Kompyuterlarni eng yangi modellariga almashtirishni o’zi kifoya qiladi degan noto’g’ri o’ylashlar ko’p tarqalgan.

Kompyuter bilan ishlaganda xavfsizlik (boshqa murakkabroq elektrotexnik vositalar bilan xam) birinchi navbatda uni to’g’ri o’rnatish va to’g’ri ekspluatatsiya qilishga bog’liq bo’ladi. Lekin ekspluatatsiya bo’yicha ko’rsatma xam Kompyuterning texnik xujjatlashtirishdagi boshqa xujjatlarda xam bu muammo xaqida axborot berilmaydi. Quyidagilarni ko’pchilik albatta inobatga olmaydi.

- PK bilan jixozlangan ish joyidagi elektromagnit maydon darajasi Kompyuter ta`minot vilkasini tarmoq razetkasiga mo’ljallanishiga bog’liq xolda 3-5 marta o’zgaradi.
- Ish joyida ko’chirma tarmoq fil trlarini ishlatishda elektromagnit maydon darajasi tez ko’tariladi.
- Statistik ma`lumotlarga qaraganda zamonaviy Kompyuterlarning 20% foizga yaqini elektromagnit maydon xosil qilish darajasi bo’yicha oldingi ishlab chiqarilgan modellaridan kamroq farq qiladi. Shuningdek, ishlatiladigan yevropa standarti bo’yicha bajarilgan elektr ta`minot razetkalari amaliyotda PK ta`minot vilkasini yerga ulovchi o’tkazgich bilan kerakli kontaktni ta`minlab bera olmaydi.
- Ish joyida displey ekranlariga o’rnatilgan past chastotali o’zgaruvchan elektr maydonni kamaytirish kafolatlangan ximoya fil trlari odatda 2-4 martadan ko’p kamaytira olmaydi.
- Ximoya fil trlarining materiallari va ularning xujjatlarida o’zgaruvchan elektromagnit maydonni kamaytirish bo’yicha ko’rsatilgan 95-99% ko’rsatkich xech qachon real sharoitda erishilmaydi. Bunday fil trlar ish joyida ekrandagi elektrostatik potentsialni kamaytirishi mumkin.
- Ixcham Kompyuterlar (noutbuk)ni ekspluatatsiyasida xam to’liq xavfsizlik ta`minlanmaydi. To’g’ri past kuchlanish iste`mol qiladigan bu Kompyuterlar ekranda elektrostatik potentsial xosil qilmasada, lekin ta`minot tizimida o’rnatilgan impul sli o’zgartkichlardan xosil bo’ladigan o’zgaruvchan

elektromagnit maydon qiymati sezilarli darajada mavjud. Xatto noutbuklarning ayrim turlaridagi elektromagnit maydon elektron nur trubkali displeylarda xosil qilinadigan maydondan unchalik kam emas

PKni ekspluatatsiya qilishda o'tkazilgan tekshiruvlar shuni ko'rsatadiki, elektromagnit xavfsizlikni ta`minlash Kompyuterlarning sifatiga bog'liq bo'lmagan xolda, o'zining ma`lum axamiyatiga ega.

Mutaxasislarning elektromagnit xavfsizlik soxasidagi ishlash malakalari shuni ko'rsatadiki, bu muammo xal qilinishi mumkin va uni xal qilishda ximoya narsa yetarli: ilmiy qo'shimcha ishlash va muammoni xal qilish usullarini tasdiqlash, mutaxasislar, o'lchov texnikalari, ximoya vositalari va xakazo. Bu borada o'z ichiga PK ekspluatatsiya bo'yicha mutaxasislarni o'qitishni mexnatni muxofaza qilish xizmati xodimlari va ShEXM bilan ishlashda xavfsizlik talablarini qondira oladigan maxsuslashtirilgan labaratoriyalarni, PK ishlatila oladigan ish joylarida baxolash usuli bo'yicha texnik vositalarni tanlashni, nurlanishni o'lchash va kamaytirish usullarini, PKdan foydalaniladigan ish joyini tashkillashtirish usullarini va optimal ish tartibini o'z ichiga oluvchi tizimli yondashish zarur. Aynan shunday kompleksli yondashish PK bilan ishlaganda ish joyida elektromagnit xavfsizlikni ta`minlaydigan na`munali dasturni taklif qiladi.

Axborot asri ko'pchilik soxalar uchun o'zining majburiyatlarini bajarish usulida dramatik o'zgarishlarga olib keldi. Xozir o'rta darajadagi texnik mutaxasis bo'lmaganlar xam ilgari yuqori darajali dasturchi qilgan ishini bajarishi mumkin. Xodim o'z ixtiyorida xech qachon ega bo'lmagan bir qancha aniq va operativ axborotlarga ega bo'ladi.

Mutaxasislarning fikri bo'yicha 50 sm masofada elektrostatik maydon ta`siri inson uchun xavfsiz darajagacha kamayadi. Maxsus ximoya fil trlarini qo'llash orqali ularni nol qiymatgacha kamaytirish mumkin. Lekin monitor ishlaganda nafaqat uning ekrani elektrlanadi, balki xona ichidagi xavo xam elektrlanishi tabiiy albatta. Bu xolda xavo o'z xolatini o'zgartiradi, ya`ni o'zida musbat zaryad to'playdi, musbat elektrlangan kislorod molekulasi inson organizmiga kisloroddek

singmaydi va nafaqat o’pkani bo’sh ishlashiga, balki o’pkaga changlarning mikroskopik zarrachalarini xam olib keladi.

Kompyuter radiatsiyasi xaqida gapiruvchi odamlar, Kompyuterni yadro reaktori bilan chalkashtirib qo’yganlar. Kompyuter xech qanday radioaktiv zarrachalar (-al fa, -beta, -gamma, neytronlar)ni chiqarmaydi. Ixtiyoriy kinoskop, monitorning kinoskopi xam rentgen nurlanishini tarqatadi, lekin zamonaviy Kompyuterlarda bu to’liqligicha neytrallanadi. Xatto eski monitorlarda xam, agar siz yarim metr uzoqroq masofada o’tirsangiz, siz to’liq xavfsizlikda bo’lasiz.

Bunday ishonch qaerda paydo bo’ldi? degan savol odamni qiziqtiradi. Bu monitorlardagi “Low Ratiation” yozuvidan xosil bo’lgan. Lekin “Radiation” o’zbek va boshqa tillarga tarjima qilinganida radiatsiya emas, balki elektromagnit nurlanish degan ma`noni beradi. Bunday nurlanishni nafaqat Kompyuter, xatto ixtiyoriy elektr asbobi xam tarqatishi tabiiy. Elektromagnit maydonni asosan monitor chiqaradi. Inson tanasi magnitlanish xususiyatiga ega va buning ta`sirida moddalar almashinuvini xam o’zgartiradi. O’zgaruvchan elektromagnit maydon inson organizmida ionlarni tebranishiga olib keladi, bu xar doim xam uning foydasiga bo’lavermaydi. Lekin, xuddi shu maydon meditsinada xam ishlatiladi (misol uchun: Fizioterapiyada), lekin u yerda xammasi ma`lum miqdorda va vaqt bo’yicha xisoblangan bo’ladi.

Ma`lumki dori bilan zaxar faqat miqdori bo’yicha farqlanadi. Lekin biz kundalik xayotda elektromagnit nurlanishni ko’p miqdorini televizordan, chang yutgichdan trolleybusdan “olamiz”, agar uyda elektr kabeli bo’lsa, bu Kompyuterdan xam zararliroq bo’ladi. Ishlayotgan monitor elektromagnit nurlanishdan tashqari elektrostatik maydonni xam xosil qiladi. Qo’lingizni monitorga yaqin olib borsangiz shitirlagan ovozni va igna kabi sanchilishlarni sezasiz. Xuddi shunday ekrandan yarim metr masofa uzoqda o’tirsangiz, siz xavfsizlikda bo’lasiz, ayniqsa ekran yerga ulangan fil tr bilan jixozlangan bo’lsa. Biroq, negadir xamma unitib qo’yadigan yana bir axamiyat bor: Monitor ishlayotgan vaqtda nafaqat ekran, balki xonadagi xavo xam zaryadlanadi. Tog’ va dengiz xavosining xususiyati ular manfiy zaryadlangan bo’ladi. Shuning uchun

momaqaldiroq bo’lib, chaqmoq chaqqandan so’ng nafas olishi yengillashadi (bu yuqoridagi sabablarga ko’ra) va aksincha, musbat zaryadlangan kislorod organizmga kislorodday singmaydi. Siz istaganingizcha xonani shamollatishingiz mumkin, lekin xavo musbat zaryadga ega bo’lsa-bu uni yo’k degani bilan tengdir.

Ko’p Kompyuterlar ishlayotgan xonada nafas olish, xar doim qiyin. Shuningdek doim televizor ishlab turadigan xonalarda nafas olish bundanda qiyinlashadi.

1. Kompyuterlar ishlayotgan xonada xavo ionizatori bo’lishi kerak.
2. Monitorni shunday qo’yish kerakki, u sizdan yarim metr uzoqroqda bo’lsin.
3. Ximoya fil trlari (elektronlari) elektromagnit nurlanishdan saqlamaydi. Rentgen nuridan, ko’zni zo’riqishidan saqlaydi (agar ximoya fil tri yerga ulangan bo’lsa).
4. Monitor elektromagnit va elektrostatik maydonni nafaqat ekran tomonidan xosil qiladi. Monitorning orqa va yon tomonlaridan xosil qilinadigan elektromagnit maydon oldi tomoniga nisbatan ancha kuchliroq. Shuning uchun, nafaqat o’zimizning monitordan, balki qo’shni monitorlardan xam ximoyalanishimiz kerak. Sanitariya me`yorlari ta`kidlaydiki, qo’shni Kompyutergacha bo’lgan masofa yarim metrdan kam bo’lmasligi kerak. Yaxshisi Kompyuterlarni devorning perimetri bo’yicha o’rnatilgani ma`qul. Afsuski, ayrim korxonalarda monitorning orqa tarafi oldinda o’tirgan odamga qarab turadi.

Xulosa qilib aytganda, xozirgi kunda Kompyuter va axborot texnologiyalarining rivojlanib borishi va turli iqtisodiy, ijtimoiy, ma`naviy soxalarga kirib borishi bajarilishi kerak bo’lgan ishlar vaqtini kamaytiradi va ularning sifatini oshiradi. Bir tomondan, Kompyuter texnikasining bunday keng yoyilishi bir qancha yutuqlarga erishishga sabab bo’lsa, ikkinchi tomondan esa, inson salomatligiga ma`lum miqdorda salbiy ta`sir qilishiga xam olib kelmoqda.

UMUMIY XULOSA

Axborot juda qadriyatli yoki o’ta muhim bo’lganligi sababli bunday axborotni saqlaydigan, qayta ishlaydigan yoki uzatadigan Kompyuter tizimlariga nisbatan turli – tuman yomon niyatli harakatlar mavjuddir. Masalan, buzg’unchi o’zini boshqa foydalanuvchi kabi ko’rsatishga intilishi, aloqa kanalini bildirmasdan eshitib olishi yoki tizim foydalanuvchilari almashayotgan axborotni ushlab olishi va o’zgartirishi mumkin. Zamonaviy Kompyuter tizimlari va tarmoqlari (KT va T), Internet yomon niyatli odamlarga muhim maxfiy axborotni o’g’irlash, buzish yoki xalaqitlarga uchratish maqsadida korxona va tashkilotlarning ichki tarmoqlariga kirish uchun ko’plab imkoniyat yaratib beradilar. Shu sababli hozirda insonlarni va jamiyatni informatsion xavfsizlik va axborotni himoya qilishni ta`minlash muammosini kompleks yechishni dolzarb ravishda kerakligi paydo bo’lmokda.

Birinchi bo’limda ma`lumotlarni uzatish tarmoqlarida axborot ximoyasini ta`minlash, boshqarish, arxitekturaviy, talablari keltirilgan. Asosiy tushuncha va atamalari, axborotni ximoya qilish talablari, ruxsat etilmagan murojaat qilish usullari, va axborotni ximoya qilish dolzarbligi, aloqa kanallarida ma`lumotlarni ximoyalash, chekkalararo ximoyalash, ulanishga mo’ljallangan usullari va bu usullardan foydalanishdagi asosiy vazifalari keltirilgan.

Ma`lumot uzatishda simsiz aloqadan foydalanish telekommunikatsiya soxasining rivojlanishidan darak beradi. Shulardan biri simsiz qurilmalarning xavfsizligini ta`minlashdir. Noutbuklar, cho’ntak Kompyuterlari, simsiz infratuzilma va uyali telefonlar shular jumlasiga kiradi.

Ikkinchi bo’limda axborotxavfsizligiga taxdidlar to’g’risida ma`lumotlar keltirilgan. Bunda asosan, tizim va tarmoqlarda taxdidlar va zaifliklar, xavfsizlikning buzilish manbalari, axborot tizimid zaif joylarning paydo bo’lishi va joylashish klassifikatsiyasi, ruxsatsiz kirishning mumkin bo’lgan asosiy usullari, axborotga shtatli murojaat qilish vositalarining turlari, Kompyuter qaroqchilari xakerlar, krakerlar to’g’risida ma`lumotlar keltirilgan.

Bundan tashqari tarmoqdagi axborotga bo’ladigan namunaviy xujumlar, tarmoqlar trafigini taxlillash, yolg’on ma`lumot yoki marshrutni kiritish, xizmat qilishdan voz kechishga undaydigan xujum vostalarining xarakteristikalari, maqsadlar va usullarga bog’liq xolda axborot xavfsizligini buzuvchilarni kategoriyalari va axborot xavfsizligini buzuvchining modeli keltirilgan.

Uchinchi bo’limda ma`lumot uzatish tarmoqlarida xavfsizlik taxdidlarini taxlili ko’rib chiqilgan. Bunda asosan tarmoqning adaptiv xavfsizligi turlari, xujumlarni aniqlash xavf-xatarlarni baxolash, ximoyalanganlikni taxlillash va xujumlarni aniqlash tizimlarining o’zaro aloqaslari, xavfsizlikni boshqarish adaptiv modellari, xujumlarni aniqlash usullar va ta`riflari, xujumlarni aniqlash tizimlarining turkumlanishi, komponentlari va arxitekturasi keltirilgan.

Ximoyalanishni taxlillash vositalari zaifliklarni topib, o’z vaqtida yo’q qilib xujumni amalga oshirishini bartaraf qiladi. Taxlil sifatida tarmoq protokollari va servislari ximoyalanishini taxlillashdan iborat. Ximoyalanishni taxlillash tizimi zaifliklarni aniqlash bo’yicha testlar seriyasini bajaradi.

FOYDALANILGAN ADABIYOTLAR

1. Domarev V.V Bezopasnost informatsionno’x texnologiy: metodologiya sozdaniya sistem zahito’ G’ V.V. Domarev. – M.: SPb; Kiev: DS DifSoft , 2001. - 688s
2. Petrakov A.V. Osnovo’ prakticheskoy zahito’ informatsii.: - M.: Radio i svyaz ., 1999 g.
3. Romanets Yu.V., Timofeev P.A., Shan gin V.F. Zahita informatsii v Kompyuterno’x tizimx i setyax.- M.: Radio i svyaz , 1999 g.
4. Kulakov M.V., Garanin A.V., Informatsionnaya bezopasnost telekommunikatsionno’x sistem (texnicheskie aspekto’) Ucheb. Posobie dlya vuzov M.: Radio i Svyaz 2004
5. Informatsionnaya bezopasnost gosudarstvenno’x organizatsiy i kommercheskix firm. Spravochnoe posobie M.: 2002.
6. Zegjda D.P. Osnovo’ bezopasnosti informatsionno’x sistem: Ucheb. posobie dlya stud. vuzov. – M.: Goryachaya liniya – Telekom, 2000. - 452s.
7. S.K. G’aniev, M.M. Karimov, K.A. Tashev “Axborot xavfsizligi” –O’quv qo’llanma – T., “Aloqachi”, 2008, 382 bet.
8. D.E Akbarov «Axborot xavfsizligini ta`minlashning kriptografik usullari va ularning qo’llanilishi» -Toshkent, “O’zbekiston markasi” nashriyoti, 2009 – 432 bet.
9. Shakina L.G. «Oxrana truda na predpriyatiyax svyazi» M: Radio i svyaz , 1983g
10. Oxrana truda na predpriyatiyax svyazi. Pod. redaktsii N.I. Baklashova. M.-1985 g.