“JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN” JURNALI
VOLUME 2, ISSUE 1, 2024. JANUARY
ResearchBib Impact Factor: 8.654/2023 ISSN 2992-8869

TARMOQLARARO EKRAN TEXNOLOGIYALARINING NAZARIY-ILMIY ASOSLARI

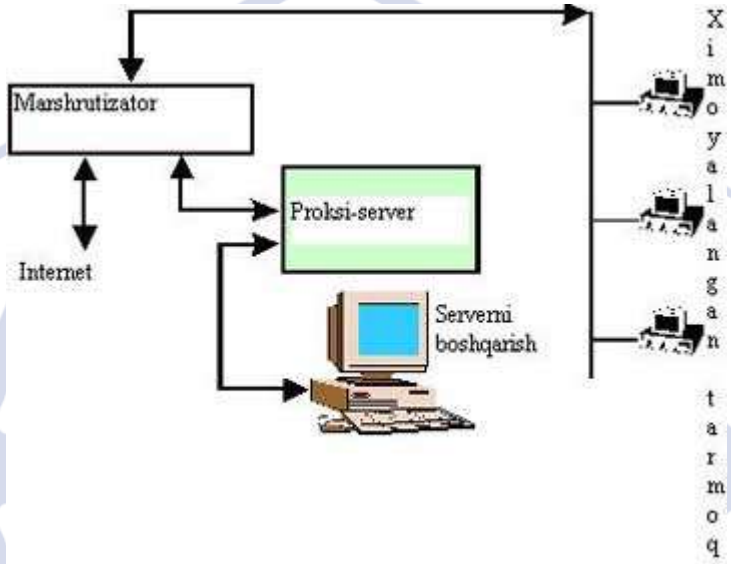
Ilmiy rahbar: i.f.d., PhD **F.T.Jumayev**
Kompyuter tizimlari va ularning dasturiy ta’minoti
yo’nalishi magistranti **Sottorov Baxtiyor Ravshan o‘g‘li**

Annotatsiya: Ushbu maqolada tarmoqlararo ekran texnologiyalarining nazariy-ilmiy asoslari haqida fikr yuritilgan hamda tarmoq xavfsizligini ta’minlash muammolari va tarmoq hujumlariga qarshi samarali himoya yechimlari haqida ma’lumot berilgan.

Kalit so’zlar: Tarmoqlararo ekran texnologiyasi va uning vazifalari, Tarmoq xavfsizligini ta’minlash muammolari va tarmoq hujumlarga qarshi samarali himoya yechimlari, Ruxsatsiz kirishni aniqlash tizimi, IDS, IPS va Firewall ning solishtirma tahlili

Tarmoqlararo ekran texnologiyasi va uning vazifalari. Tarmoqlararo ekran — himoyalash vositasi bo‘lib, ishonchli tarmoq, va ishonchsiz tarmoq orasida ma’lumotlarga kirishni boshqarishda qo‘llaniladi. Tarmoqlararo ekran ko‘p komponentli bo‘lib, u Internetdan tashkilotning axborot zahiralarini himoyalash strategiyasi sanaladi. Ya’ni tashkilot tarmog‘i va Internet orasida qo‘riqlash vazifasini bajaradi. Tarmoqlararo ekranning asosiy funksiyasi ma’lumotlarga egalik qilishni markazlashtirilgan boshqaruvini ta’minlashdan iborat. Tarmoqlararo ekran quyidagi himoyalarni amalga oshiradi: o‘rinsiz trafiklar, ya’ni tarmoqda uzatiladigan xabarlar oqimini taqiqlash; qabo‘l qilingan trafikni ichki tizimlarga yunaltirish; ichki tizimning zaif qismlarini yashirish bilan Internet tomonidan uyushtiriladigan xujumlardan himoyalash; barcha trafiklarni bayonlashtirish; ichki ma’lumotlarni, masalan tarmoq topologiyasini, tizim nomlarini, tarmoq uskunalarini va foydalanuvchilarning identifikatorlarini Internetdan yashirish; ishonchli autentifikatsiyani taьminlash. Ko‘pgina adabiyotlarda tarmoqlararo ekran tushunchasi brandmauer yoki FireWall deb yuritilgan. Umuman bo‘larning xammasi yagona tushunchadir. Tarmoqlararo ekran — bu tizim, umumiy tarmoqni ikki qismga ajratib, tarmoqlararo himoya vazifasini o‘taydi va ma’lumotlar paketining

chegaradan o‘tish shartlarini amalga oshiradigan qoidalar to‘plami hisoblanadi. Odatda tarmoqlararo ekran ichki tarmoqlarni global tarmoqlardan, ya’ni Internetdan himoya qiladi. SHuni aytish kerakki, tarmoqlararo ekran nafaqat Internetdan, balki korporativ tarmoqlardan xam himoya qilish qobiliyatiga egadir.



1-rasm. Firewallga asosida qurilgan tarmoq tuzilishi

Har qanday tarmoqlararo ekran ichki tarmoqlarni to‘liq himoya qila oladi deb bo‘lmaydi. Internet xizmati va hamma protokollarning amaliy jihatdan axborotlarga nisbatan himoyasining to‘liq bo‘lmaganligi muammosi bor. Bu muammolar kelib chiqishining asosiy sababi Internetning UNIX operatsion tizim bilan bog‘liqligida. TCP/IP (Transtnission Control Protokol/lnternet Protocol) Internetning global tarmog‘ida kommunikatsiyani ta’minlaydi va tarmoqlarda ommaviy ravishda qo‘llaniladi.

Tarmoq xavfsizligini ta’minlash muammolari va tarmoq hujumlarga qarshi samarali himoya yechimlari. Mamlakatimiz siyosatining ustuvor yo‘nalishlariga kiritilgan kompyuter va axborot texnologiyalari, telekomunikatsiya, ma’lumotlarni uzatish tarmoqlari, Internet xizmatlaridan foydalanish rivojlanmoqda

va modernizatsiyalashmoqda. Jamiyatimizning barcha sohalariga kundalik hayotimizga zamonaviy axborot texnologiyalarini keng joriy etish istiqboldagi maqsadlarimizga erishishni ta’minlaydi. Har bir soha faoliyatida Internet tarmog‘idan foydalanish ish unumdorligini oshirmoqda.

Aynan tarmoqdan foydalangan holda tezkor ma’lumot almashish vaqtdan yutish imkonini beradi. Xususan, yurtimizda Elektron hukumat tizimi shakllantirilishi va uning zamirida davlat boshqaruv organlari hamda aholi o‘rtasidagi o‘zaro aloqaning mustahkamlanishini tashkil etish tarmoqdan foydalangan holda amalga oshadi. Tarmoqdan samarali foydalanish demokratik axborotlashgan jamiyatni shakllantirishni ta’minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha tezkor natijaga ega bo‘linadi.

Biroq tarmoqqa noqonuniy kirish, axborotlardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi. Ish faoliyatini tarmoq bilan bog‘lagan korxona, tashkilotlar hamda davlat idoralari ma’lumot almashish uchun tarmoqqa bog‘lanishidan oldin tarmoq xavfsizligiga jiddiy e’tibor qaratishi kerak. Tarmoq xavfsizligi uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotni ishonchli tizimli tarzda ta’minlash maqsadida turli vositalar va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirish orqali amalga oshiriladi. Tarmoq xavsizligini ta’minlash maqsadida qo‘llanilgan vosita xavf-xatarni tezda aniqlashi va unga nisbatan qarshi chora ko‘rishi kerak. Tarmoq xavfsizligiga tahdidlarning ko‘p turlari bor, biroq ular bir necha toifalarga bo‘linadi:

1. axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (Eavesdropping);
2. xizmat ko‘rsatishdan voz kechish; (Denial-of-service)
3. portlarni tekshirish (Port scanning).

Axborotni uzatish jarayonida, eshitish va o‘zgartirish hujumi bilan telefon aloqa liniyalari, internet orqali tezkor xabar almashish, videokonferensiya va faks jo‘natmalari orqali amalga oshiriladigan axborot almashinuvida foydalanuvchilarga

sezdirmagan holatda axborotlarni tinglash, o‘zgartirish hamda to‘sib qo‘yish mumkin. Bir qancha tarmoqni tahlillovchi protokollar orqali bu hujumni amalga oshirish mumkin. Hujumni amalga oshiruvchi dasturiy ta’minotlar orqali CODEC (video yoki ovozli analog signalni raqamli signalga aylantirib berish va aksincha) standartidagi raqamli tovushni osonlik bilan yuqori sifatli, ammo katta hajmni egallaydigan ovozli fayllar (WAV)ga aylantirib beradi. Odatda bu hujumning amalga oshirilish jarayoni foydalanuvchiga umuman sezilmaydi. Tizim ortiqcha zo‘riqishlarsiz va shovqinsiz belgilangan amallarni bajaraveradi. Axborotning o‘g‘irlanishi haqida mutlaqo shubha tug‘ilmaydi. Faqatgina oldindan ushbu tahdid haqida ma’lumotga ega bo‘lgan va yuborilayotgan axborotning o‘z qiymatini saqlab qolishini xohlovchilar maxsus tarmoq xafvsizlik choralarini qo‘llash natijasida himoyalangan tarmoq orqali ma’lumot almashish imkoniyatiga ega bo‘ladilar. Tarmoq orqali ma’lumot almashish mobaynida yuborilayotgan axborotni eshitish va o‘zgartirishga qarshi bir necha samarali natija beruvchi texnologiyalar mavjud:

1. IPSec (Internet protocol security) protokoli;
2. VPN (Virtual Private Network) virtual xususiy tarmoq;
3. IDS (Intrusion Detection System) ruxsatsiz kirishlarni aniqlash tizimi.

Ipsec (Internet protocol security) bu xavfsizlik protokollari hamda shifrlash algoritmlaridan foydalangan holda tarmoq orqali xavfsiz ma’lumot almashish imkonini beradi. Bu maxsus standart orqali tarmoqdagi kompyuterlarning o‘zaro aloqasida dastur va ma’lumotlar hamda qurilmaviy vositalar bir-biriga mos kelishini ta’minlaydi. Ipsec protokoli tarmoq orqali uzatilayotgan axborotning sirliligini, ya’ni faqatgina yubo-ruvchi va qabul qiluvchiga tushunarli bo‘lishini, axborotning sofligini hamda paketlarni autentifikatsiyalashni amalga oshiradi. Zamonaviy axborot texnologiyalarni qo‘llash har bir tashkilotning rivojlanishi uchun zaruriy vosita bo‘lib qoldi, Ipsec protokoli esa aynan quyidagilar uchun samarali himoyani ta’minlaydi:

- bosh ofis va filiallarni global tarmoq bilan bog‘laganda;
- uzoq masofadan turib, korxonani internet orqali boshqarishda;
- homiylar bilan bog‘langan tarmoqni himoyalashda;
- elektron tijoratning xavfsizlik darajasini yuksaltirishda.

Ruxsatsiz kirishni aniqlash tizimi. Ruxsatsiz kirishni aniqlash tizimi (IDS) yordamida tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi. Ruxsatsiz kirishlarni aniqlash tizimlari deyarli chorak asrlik tarixga ega. Ruxsatsiz kirishlarni aniqlash tizimlarining ilk modellari va prototiplari kompyuter tizimlarining audit ma’lumotlarini tahlillashdan foydalangan. Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi.

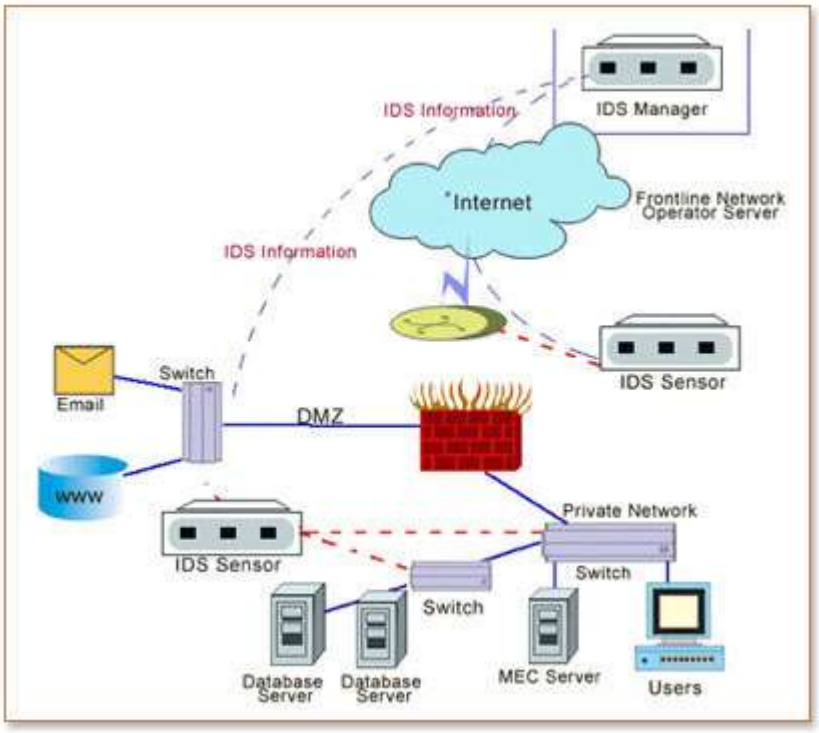
DS tizimlari arxitekturasi tarkibiga quyidagilar kiradi:

- himoyalangan tizimlar xavfsizligi bilan bog‘liq holatlarni yig‘ib tahlillovchi sensor qism tizimi;
- sensorlar ma’lumotlariga ko‘ra shubhali harakatlar va hujumlarni aniqlashga mo‘ljallangan tahlillovchi qism tizimi;
- tahlil natijalari va dastlabki holatlar haqidagi ma’lumotlarni yig‘ishni ta’minlaydigan omborxona;
- IDS tizimini konfiguratsiyalashga imkon beruvchi, IDS va himoyalangan tizim holatini kuzatuvchi, tahlil qism tizimlari aniqlagan mojarolarni kuzatuvchi boshqaruv konsoli. Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi.

Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (NIDS) ishlash tamoyili quyidagicha:

1. tarmoqqa kirish huquqiga ega bo‘lgan trafiklarni tekshiradi;
2. zararli va ruxsatga ega bo‘lmagan paketlarga cheklov qo‘yadi.

Research Science and Innovation House



2-rasm. IDS tizimiga asoslangan tarmoq tuzilishi

IPS – (Intrusion Prevention System) esa kompyuter tizimlari yoki tarmoqlarida yuz berayotgan hodisalarni kuzatish va kompyuter xavfsizligi siyosati yoki standart xavfsizlik qoidalarini buzishga olib keladigan holatlarning tahlili bilan birgalikda aniqlangan holatlarni to'xtatishga, hujumlarga qarshi javob qaytarish qobiliyatli harakatlar yig'indisidir.

IPS texnologiyasi IDS texnologiyasini mustaqil ravishda nafaqat xavfni aniqlabgina qolmay, balki uni muvaffaqiyatli bloklashi bilan to'ldiradi. Ushbu taxminiy IPS funktsiyasi IDSga qaraganda ancha kengroq:

- IPS hujumni bloklaydi (xavfsizlik siyosatini buzadigan, resurslarga, hostlarga, dasturlarga kirishni taqiqlovchi foydalanuvchi sessiyasining to‘xtatilishi);
- IPS himoyalangan muhitni o‘zgartiradi (hujumlarni oldini olish uchun tarmoq qurilmalarini qayta tuzish);
- IPS hujum tarkibini o‘zgartiradi (masalan, virusi bilan yuborilgan faylni xatdan olib tashlaydi va uni allaqachon tozalagan yoki proksi-server sifatida yuboradi, kiruvchi so‘rovlarni tahlil qiladi va paketli sarlavhalarda ma'lumotni tashlab ketadi).

Biroq, bu tizimlar aniq afzalliklaridan tashqari, ularning kamchiliklariga ham ega. Masalan, IPS har doim axborot xavfsizligi intsidentini aniq belgilab bera olmaydi, yoki xatti-harakatlarning odatdagi xatti-harakatlarini noto‘g‘ri qabul qiladi yoki foydalanuvchini hodisa sifatida qabul qiladi. Birinchi variantda yolg‘on salbiy hodisa haqida gapirish odatiy holdir, ikkinchi variantda esa noto‘g‘ri ijobiy hodisalar aytiladi. Shuni esda tutish kerakki, ularning paydo bo‘lishini to‘liq bartaraf etishning iloji yo‘q, shuning uchun tashkilot har bir holda ikki guruhning qaysi xavfini kamaytirish yoki qabul qilish kerakligini mustaqil ravishda hal qilishi mumkin.

IPS texnologiyasidan foydalangan holda hodisalarni aniqlashning turli usullari mavjud. Ko‘pgina IPS ilovalari ushbu texnologiyalarning summasini ko‘proq xavf tahdidini ta'minlash uchun foydalanadi.

IDS, IPS va Firewall ning solishtirma tahlili. IDS va Firewall ham tarmoq xavfsizligi bilan shug‘ullansada, IDS xavfsizlik devoridan farq qiladi, buning sababi, xavfsizlik devorlari ularni to‘xtatish uchun hujumlarni ko‘rib chiqadi. Xavfsizlik devori kirishlarni oldini olish uchun tarmoqlar orasidagi ulanishni cheklaydi va tarmoq ichidagi hujumni bildirmaydi. IDS sodir bo‘lganidan keyin shubhali hujumni baholaydi va signalni signallaydi. IDS shuningdek, tizim ichida yuzaga kelgan hujumlarni ham kuzatib boradi. Tarmoqqa asoslangan kirishni himoyalash tizimi xavfsizlik devorining soddalashtirilgan filtrlash qoidalari e'tiborga olinmasligi uchun mo‘ljallangan zararli paketlarni ham aniqlay oladi.

IDS xavfsizlik devori yoki yaxshi antivirus dasturini almashtirish emas. IDS sizning tizimingizda maxsus yoki tarmoq xavfsizligini oshirish uchun standart xavfsizlik mahsulotlari (antivirus va xavfsizlik devori kabi) bilan birgalikda foydalanish uchun vosita sifatida qaralishi kerak.

FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. Основы криптографии: Учебное пособие. – М., 2002
3. Арипов М. , Пудовченко Ю. Е., Арипов М. Основы Интернет. – Т., 2003.
4. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
5. Давыдов А.С., Маслова Т.В. Информационные технологии в деятельности органов внутренних дел: Учебное пособие. – Челябинск, 2007.
6. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программноаппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.
7. Информационные технологии управления в органах внутренних дел: Учебник / Под ред. доцента Ю.А. Кравченко. – М., 1998.
8. Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.
9. Казиев В.М. Введение в правовую информатику. – http://www. intuit.ru.

Research Science and Innovation House