TARMOQ HUJUMLARIDAN HIMOYALANISHNING ZAMONAVIY TIZIMLARI VA TEXNOLOGIYALARI

Samatov Boburmirzo Xamidillo o‘g‘li
Andijon davlat universiteti
Axborot texnologiyalari o‘qituvchisi
boburmirzosamatov@adu.uz
Sharobidinov Qudratillo Kamoldin o‘g‘li
Andijon davlat universiteti Axborot havfsizligi yo’nalishi1-kurs talabasi
bobca98@gmail.com

Annotatsiya: Mazkur maqolada tashkilot tarmog‘ini internetdan himoya qilishning muhim vositasi — tarmoqlararo ekran (firewall) tushunchasi va uning asosiy funksiyalari yoritilgan. Tarmoqlararo ekran ma’lumotlarga markazlashtirilgan boshqaruvni ta’minlab, ruxsatsiz trafiklarni bloklaydi, ichki tizimlarni himoya qiladi hamda trafikni tahlil qiladi. TCP/IP protokolining zaif tomonlari va elektron pochta orqali xaker hujumlari xavfi ham muhokama qilingan. Amaliy darajadagi shlyuzlar va ularning xavfsizlikni oshirishdagi roli ko‘rsatilib, System Security Scanner (SSS) dasturi orqali Unix tizimidagi xavflarni aniqlash imkoniyatlari sanab o‘tilgan. Shuningdek, shifrlash algoritmlari, raqamli sertifikatlar, trafik tahlili va monitoring vositalari haqida keng qamrovli tushunchalar berilgan. Material axborot xavfsizligini ta'minlashda qo‘llaniladigan texnik, tashkiliy va huquqiy choralar bilan tanishtiradi hamda O‘zbekiston Respublikasidagi monitoring institutlari faoliyati haqida ham ma’lumot beradi. Ushbu ma’lumotlar kiberxavfsizlik sohasida tahdidlarni aniqlash va ularga qarshi samarali choralar ko‘rishda muhim ahamiyatga ega.

Kalit so‘zlar: Firewall, Brandmauer, TCP/IP, SMTP, System Security Scanner (SSS), oimmetrik shifrlash, oqimli shifrlash, ochiq kalit, tarmoq monitoring, axborot xavfsizligi, foydalanuvchi autentifikatsiyasi, ma’lumotni shifrlab uzatish, axborot topologiyasi.

Tarmoqlararo ekran ko‘p komponentli bo‘lib, u Internetdan tashkilotning axborot zaxiralarini himoyalash strategiyasi sanaladi. Ya’ni tashkilot tarmog‘i va Internet orasida qo‘riqlash vazifasini bajaradi.

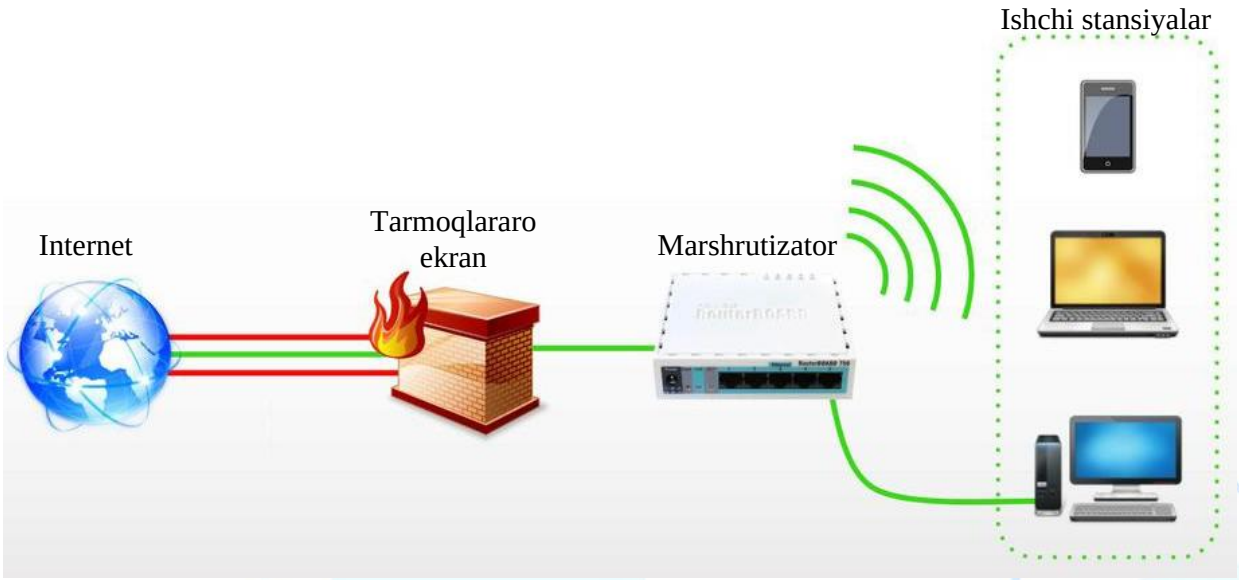
Tarmoqlararo ekranning asosiy funksiyasi ma’lumotlarga egalik qilishni markazlashtirilgan boshqaruvini ta’minlashdan iborat.

Tarmoqlararo ekran quyidagi himoyalarni amalga oshiradi:

– o‘rinsiz trafiklar, ya’ni tarmoqda uzatiladigan xabarlar oqimini taqiqlash;
– qabul qilingan trafikni ichki tizimlarga yo‘naltirish;
– ichki tizimning zaif qismlarini yashirish bilan Internet tomonidan uyushtiriladigan hujumlardan himoyalash;
– barcha trafiklarni bayonlashtirish;
– ichki ma’lumotlarni, masalan tarmoq topologiyasini, tizim nomlarini, tarmoq uskunalarini va foydalanuvchilarning identifikatorlarini Internetdan yashirish;
– ishonchli autentifikatsiyani ta’minlash.

Ko‘pgina adabiyotlarda tarmoqlararo ekran tushunchasi brandmauer yoki Fire Wall deb yuritilgan. Umuman bularning hammasi yagona tushunchadir.

TCP/IP (Transmission Control Protocol/Internet Protocol) Internetning global tarmog‘ida kommunikatsiyani ta’minlaydi va tarmoqlarda ommaviy ravishda qo‘llaniladi, lekin ular ham himoyani yetarlicha ta’minlay olmaydi, chunki TCP/IP paketining boshida xaker hujumi uchun qulay ma’lumot ko‘rsatiladi.



1-rasm. Tarmoqlararo ekranlarning ulanish sxemasi

Internetda elektron pochtani jo‘natishni oddiy protokol — pochta transport xizmati amalga oshirad (SMTP — Simple Mail Transfer Protocol). Bu protokolda mavjud bo‘lgan himoyalashning muhim muammolaridan biri — foydalanuvchi jo‘natuvchining manzilini ko‘ra olmasligidir. Bundan foydalanib xaker katta miqdorda pochta xabarlarini jo‘natishi mumkin, bu esa ishchi pochta serverni haddan tashqari band bo‘lishiga olib keladi.

Tarmoq servislariga kirish siyosati, odatda, quyidagi prinsiplarga moyil bo‘ladi:

– Internetdan ichki tarmoqqa kirishni taqiqlash, lekin ichki tarmoqdan Internetga kirishga ruxsat berish;
– vakolatlangan tizimlarga Internet dan ichki tarmoqqa cheklanilgan kirishga ruxsat berish.

Amaliy darajadaga shlyuzlar mijoz va tashqi xost-kompyuter bilan to‘g‘ridan-to‘g‘ri aloqa o‘rnatishga yo‘l qo‘ymaydi. Shlyuz keladigan va jo‘natiladigan paketlarni amaliy darajada filtrlaydi.

Server-dallollar shlyuz orqali aniq server tomonidan ishlab chiqilgan ma’lumotlarni qaytadan yo‘naltiradi.

Amaliy darajadagi shlyuzlar nafaqat paketlarni filtrlash, balki serverning barcha ishlarini qayd qilish va tarmoq administratorini noxush ishlardan xabar qilish imkoniyatiga ham ega.

Amaliy darajadaga shlyuzlarning afzalliklari quyidagilardan iborat:

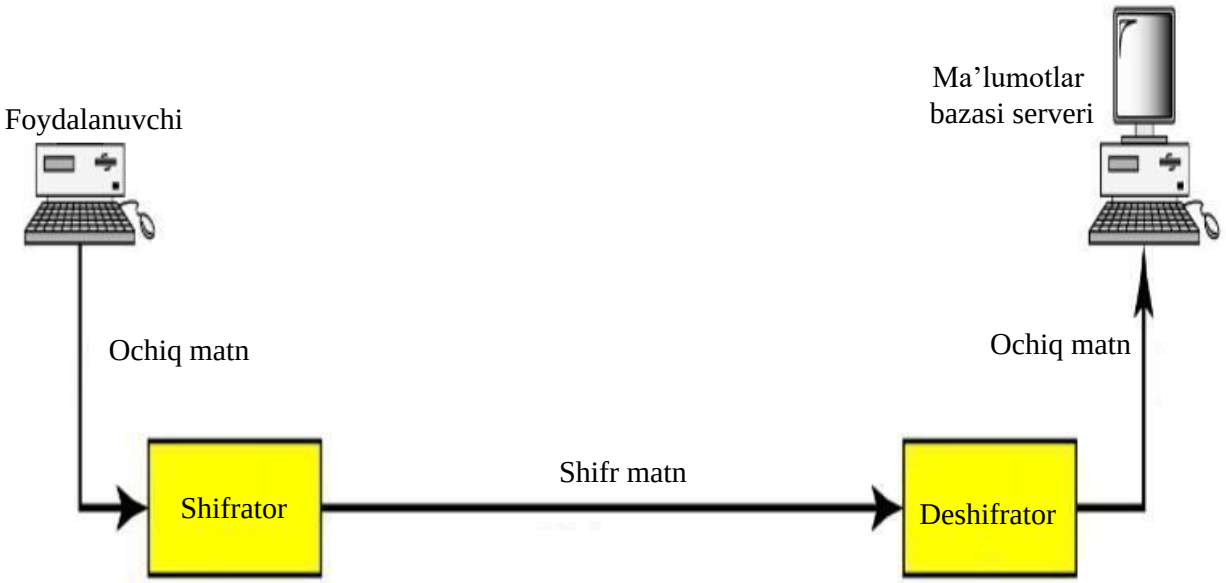
– global tarmoq tomonidan ichki tarmoq tarkibi ko‘rinmaydi;
– ishonchli autentifikatsiya va qayd qilish;
– filtrlash qoidalarining yengilligi;
– ko‘p tamoyilli nazoratlarni amalga oshirish mumkinligi.

SSS (System Security Scanner) dasturi. Ushbu dastur Unix operatsion tizimi o‘rnatilgan kompyuterlarda xavfsizlik holatini tekshirish va operatsion tizimning tashqi hamda ichki zaif qismlarini aniqlashga yo‘naltirilgan. Bundan tashqari u kirish huquqlarini, fayllarga egalik qilish huquqlarini, tarmoq zaxiralarini konfiguratsiyalashni, autentifikatsiyalash dasturlarini va boshqalarni tekshirishi mumkin.

Dasturning quyidagi imkoniyatlari mavjud:

– konfiguratsiyani tekshirish, ya’ni ruxsatsiz kirishlarning oldini olish maqsadida konfiguratsiyani tekshirish. Bunga quyidagilar kiradi: konfiguratsiya fayllari, operatsion tizim versiyasi, kirish huquqlari, foydalanuvchilarning zaxiralari, parollar;
– tizimdagi xavfli o‘zgarishlarni tekshirish. Ruxsatsiz kirishlar oqibatida tizimda sodir bo‘lgan o‘zgarishlarni qidirishda qo‘llaniladi. Bunday o‘zgarishlarga quyidagilar kiradi: fayllar egallagan xotira hajmining o‘zgarishi, ma’lumotlarga kirish huquqi yoki fayldagi ma’lumotlarning o‘zgarishi, foydalanuvchilarning zaxiralarga kirish parametrlarining o‘zgarishi, fayllarni ruxsatsiz boshqa bir tashqi kompyuterlarga uzatishlar;
– foydalanuvchi interfeysining qulayligi. Bu interfeys yordamida nafaqat dastur bilan qulay ishlash ta’minlanadi, balki bajarilgan ishlar bo‘yicha hisobotlar ham yaratiladi;
– masofadan skanerlash. Tarmoqdagi kompyuterlarni tekshirish va aloqa jarayonida ma’lumotlarni shifrlash imkoniyati ta’minlanadi;
– hisobotlar tuzish. Bajarilgan ishlar bo‘yicha to‘liq hisobotlar yaratiladi. Ushbu hisobotlarda tizimning aniqlangan zaif bo‘g‘inlarining izohi

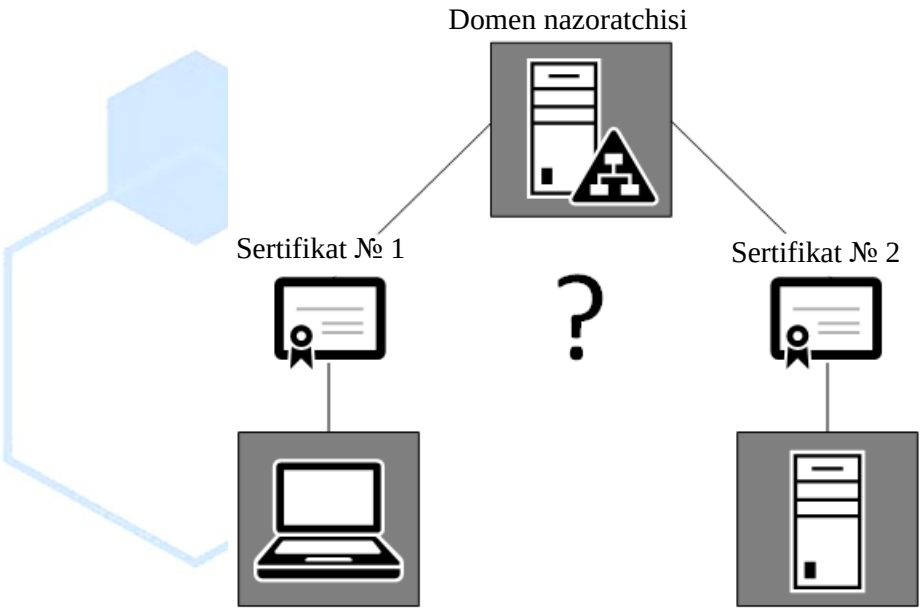
keltiriladi va ularni tuzatish bo‘yicha ko‘rsatmalar beriladi. Hisobot HTML yoki oddiy matn ko‘rinishida bo‘lishi mumkin.



2-rasm. Ma’lumotni shifrlab uzatish sxemasi

Shifrlash. Axborotdagi belgilarni ma’lum bir matematik amallar va usullar yordamida qayta akslantirish shifrlash jarayoni hisoblanadi. Axborotlarni shifrlashda asosan simmetrik blokli shifrlash algoritmlari qo’llaniladi. Uzluksiz ma’lumotlar uchun esa, oqimli shifrlash algoritmlari qo’llanilishi mumkin. 2.9-rasmda ma’lumotlarni shifrlash sxemasi keltirilgan.

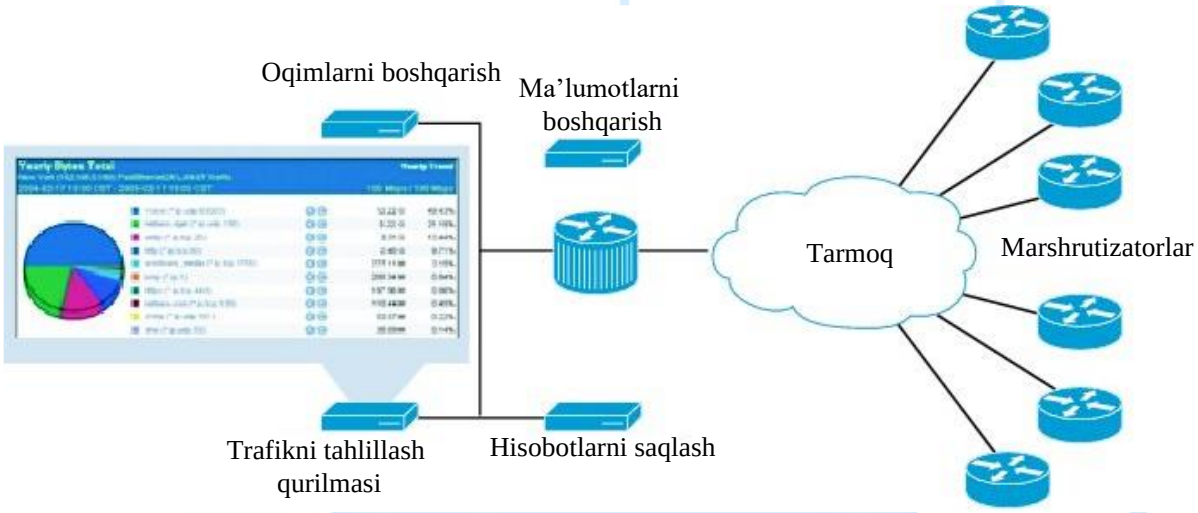
Sertifikatlarni o’rnatish. Raqamli sertifikatlar ishlatilganida kompyuter tarmog’i foydalanuvchilari xususidagihyech qanday axborotni saqlamaydi. Bunday axborotni foydalanuvchilarning o’zi so’rov-sertifikatlarida taqdim etadilar. Bunda maxfiy axborotni, xususan maxfiy kalitlarni saqlash vazifasi foydalanuvchilarning o’ziga yuklanadi.Foydalanuvchi shaxsini tasdiqlovchi raqamli sertifikatlar foydalanuvchilar so’rovi bo’yicha maxsus vakholatli tashkilot-sertifikasiya markazi CA tomonidan, ma’lum shartlar bajarilganida beriladi. Ta’kidlash lozimki, sertifikat olish muolajasining o’zi xam foydalanuvchining haqiqiyligini tekshirish bosqichini o’z ichiga oladi. Bunda tekshiruvchi taraf sertifikasiyalovchi tashkilot bo’ladi. Sertifikat olish uchun mijoz sertifikasiya markaziga shaxsini tasdiqlovchi ma’lumotni va ochiq kalitini taqdim etishi lozim.



3-rasm. Sertifikatlarni qo’llash sxemasi

Ochiq kalitlarning sertifikatlar bilan uzviy bog’liqligini alohida ta’kidlash lozim. Sertifikat nafaqat shaxsni, balki ochiq kalit mansubligini tasdiqlovchi xujjatdir. Raqamli sertifikat ochiq kalit va uning egasi o’rtasidagi moslikni o’rnatadi va kafolatlaydi. Bu ochiq kalitni almashtirish xavfini bartaraf etadi.

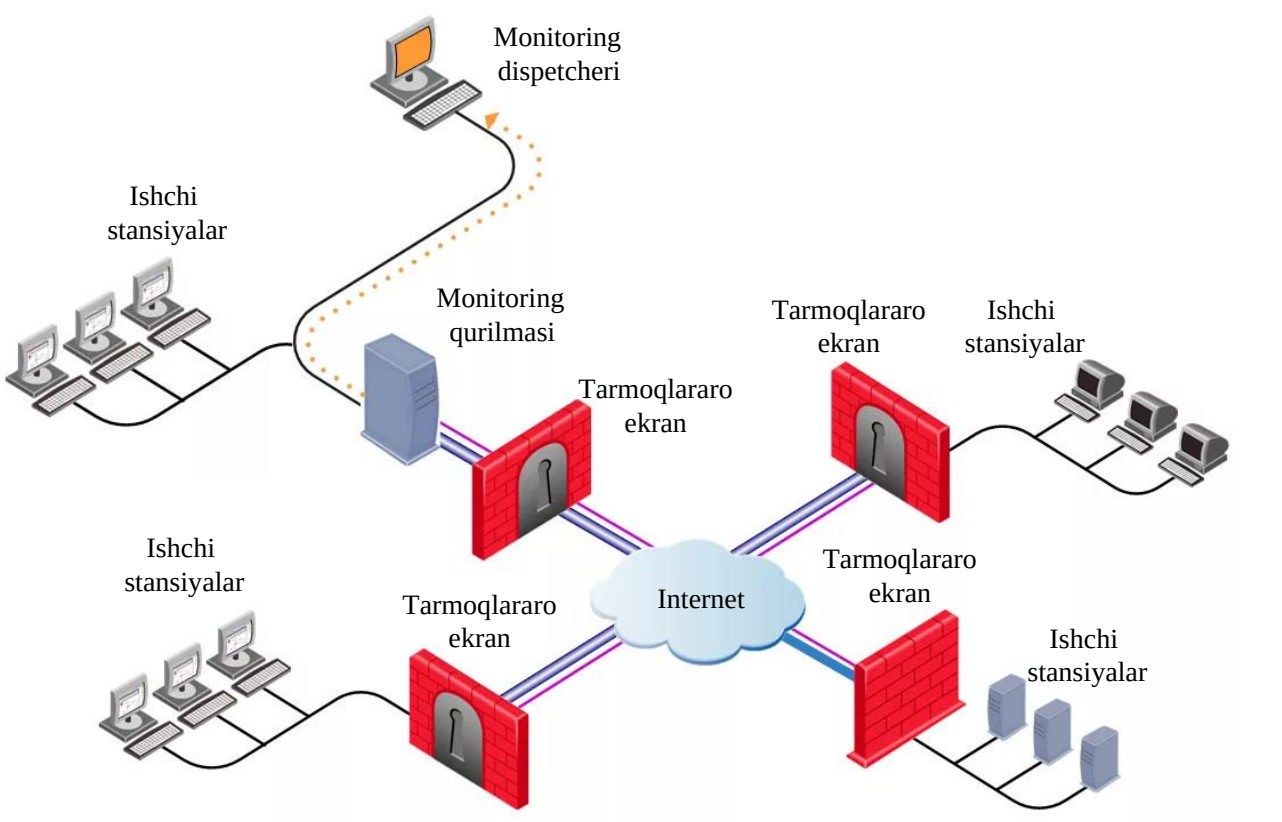
Trafikni tahlillash. Tarmoqlarni tahlillash dasturlari va qurilmalari tarmoqni berilgan qonun-qoidalar asosida tahlillashga bag’ishlangandir. U o’rnatilgan tarmoqda qanday axborotlar kirib kelgani va chiqib ketganini paketlar asosida tahlildan o’tkazadi. Agar begona paket aniqlansa, unda u haqida ma’murga xabar beradi.



4-rasm. Tarmoq trafigini tahlillash

Monitoring. Ma’lumki, axborot-kommunikasiya tizimlari har xil texnologik jarayonlarni yoki uning qismini amalga oshiradi. Ravshanki, axborot oqimlari harakatidagi har qanday yanglishish yoki ulardan foydalanish qoidalarining buzilishi ishdagi muammolarga va qo’shimcha harajatlarga yoki foydaning boy berilishiga olib kelishi mumkin. Shuning uchun, har qanday bank AXT xavfsizlik bo’limiga kuchli etibor beradi.

O‘zbekistonda Respublika Oliy Majlisi huzurida maxsus Amaldagi qonun hujjatlari monitoringi instituti faoliyat ko‘rsatadi. Keyingi vaqtda ommaviy axborot vositalari M.i ham tashkil qilindi. Bu ishni O‘zbekiston matbuot va axborot agentligi tarkibida tuzilgan (2002 yil 3 iyul) Ommaviy axborot vositalari monitoringi va ularni litsenziyalash markazi amalga oshiradi.



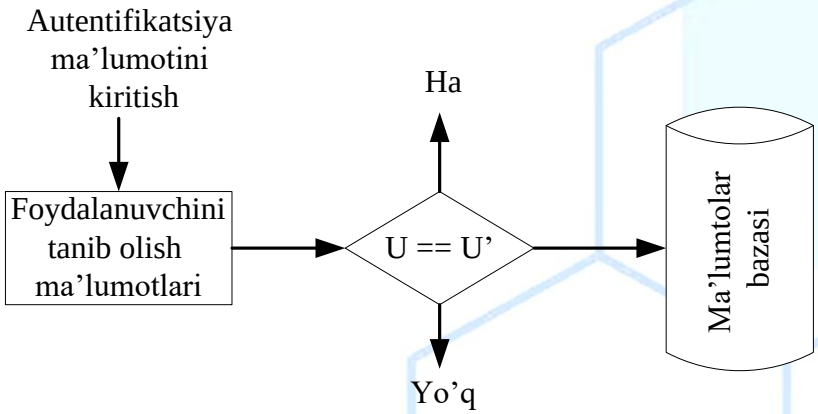
5-rasm. Tarmoq monitoringini amalga oshirish

Internet tarmog’i orqali umumiy kanal hosil qilingan bir nechta local tarmoqlarning aynan bittasida monitoring qurilmasi o’rnatilgan va u monitoring dispetcheri yordamida boshqarilib turadi.

Identifikatsiya.Identifikatsiya foydalanuvchilarni tanib olish jarayoni hisoblanadi. Tizimga ulangan foydalanuvchi o'zining nomi, mahfiy so'zi, ID va smart kartalari hattoki, biometrik parametrlari: ko'z, yuz, barmoq izi, ko'z qorachig'i, DNK, ovoz va boshqalari orqali identifikatsiyalanishi mumkin.

Tizim tomonidan tanib olingan foydalanuvchining haqiqiyligini tekshirish muammosi yuzaga kelsa, autentifikatsiya yordamida amalga oshiriladi.

Autentifikatsiya.Tanib olingan foydalanuvchini haqiqiyligini tekshirishda autentifikatsiyalash usullaridan foydalaniladi. Autentifikatsiyalash usulining ham identifikatsiyalash kabi, mahfiy so'zi, ID va smart kartalari hattoki, biometrik parametrlari: ko'z, yuz, barmoq izi, ko'z qorachig'i, DNK, ovoz asosida kabi usullari mavjud. Foydalanuvchi tanib olinadi va bazada mavjudligi tekshiriladi. Agar tanib olingan foydalanuvchining autentifikatori uning identifikatoriga mos bo'lsa, demak, foydalanuvchi haqiqiy hisoblanadi.



6-rasm. Autentifikatiya jarayonini amalga oshirish

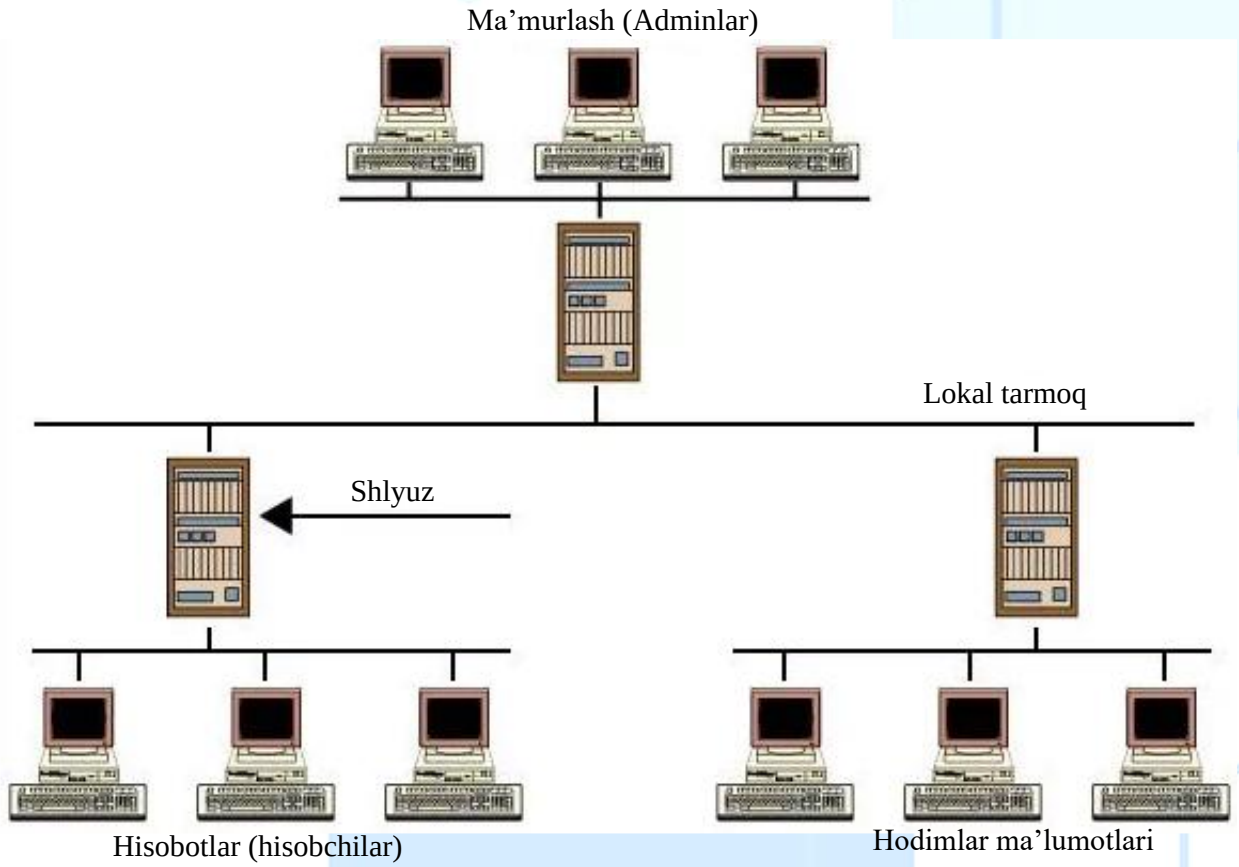
Avtorizatsiy. Kompyutyer tizimlari, ma'lumotlar bazasi va serverdan foydalanishda foydalanuvchilar guruhi yoki aynan bitta odamga o'zining huquqi doirasida amallar bajarish avtorizatsiya orqali amalga oshiriladi. Yoki tizimdan foydalanish huquqi faqatgina avtorizatsiyalangan foydalanuvchilarga taqdim etiladi.

Avtorizatsiyalash yuqorida aytib o'tilganidek, ma'lumotlar bazasining himoyalash modellari: rolli, mandatli, diskretsion, Pell-La-Padula yoki mujassamlashgan modellar asosida amalga oshiriladi.

Avtorizatsiyalash samaradorligini oshirish maqsadida qo'shimcha ravishda kontekst, panjara va o'zgaruvchilar asosida ruhsatlarni nazoratlash modellari ham keng qo'llaniladi.

Ma'murlash. Tizim yoki tarmoqni xavfsizlik nuqtai nazaridan boshqarish va uni nazoratlash ma'murlash yordamida amalga oshiriladi. Ko'pchilik adabiyotlarda ushbu vazifalarni admin amalga oshiradi. Ma'lumotlar bazasidan kelib chiqib turli turdagi adminlar farqlanadi.

Foydalanuvchining tarmoqdagi xarakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish. Ushbu xisobot axboroti xavfsizlik nuqtai nazaridan tarmoqdagi xavfsizlik xodisalarini oshkor qilish, taxlillash va ularga mos reaktsiya ko'rsatish uchun juda muximdir.



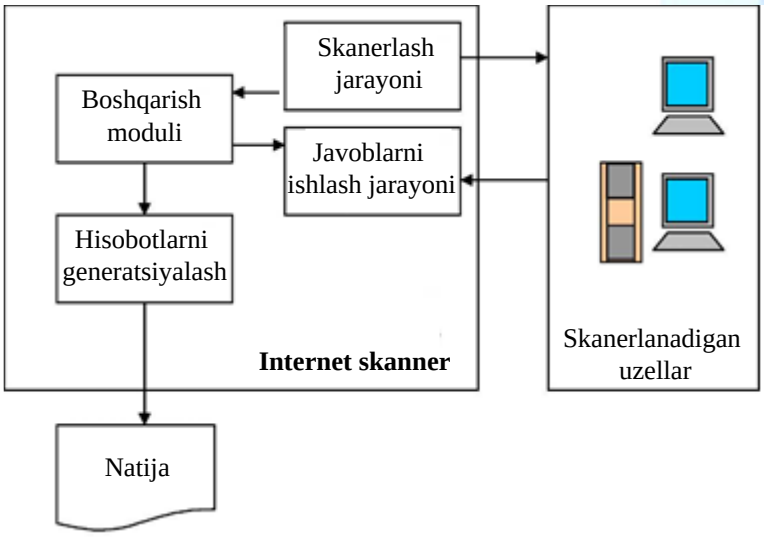
7-rasm. Tizimni boshqarish adminlari

Hujumlar tasnifini hujumlar ro'yxati yoki hujumlar matritsasi yordamida amalga oshirish mumkin. Bu usullarning har biri matritsa yoki ro'yhat elementini aniqlashni ko'zda tutadi. Bu ayrim hujumlar uchun maqbul taksonomiyaning olti hususiyatini

qanoatlantiruvchi tavfsifning mavjud emasligiga olib kelishi mumkin, bu esa o’z navbatida hujumning noto’g’ri tasniflanishiga olib kelishi mumkin. Bu holda, maxsus tavsifni yoki ba’zi bir umumiy hujum guruhini, masalan, "tasniflanmagan hollar" hujumlari guruhini ishlatish mumkin.

Himoyalanishni taxlillash.Himoyalanishni taxlillash vositalari zaifliklarni topib va o’z vaqtida yo’q qilib xujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatilishiga bo’ladigan barcha sarfharajatlar kamayadi.

Himoyalanishni taxlillash vositalari tarmoq sathida, operaqion tizim sathida va ilovalar sathida ishlashi mumkin. Ular tekshirishlar so nini borabora ko’paytirish, axborot tizimiga "ichkarilab borish" va uning barcha sathlarini tadqiqlash orqali zaifliklarni qidirishi mumkin.

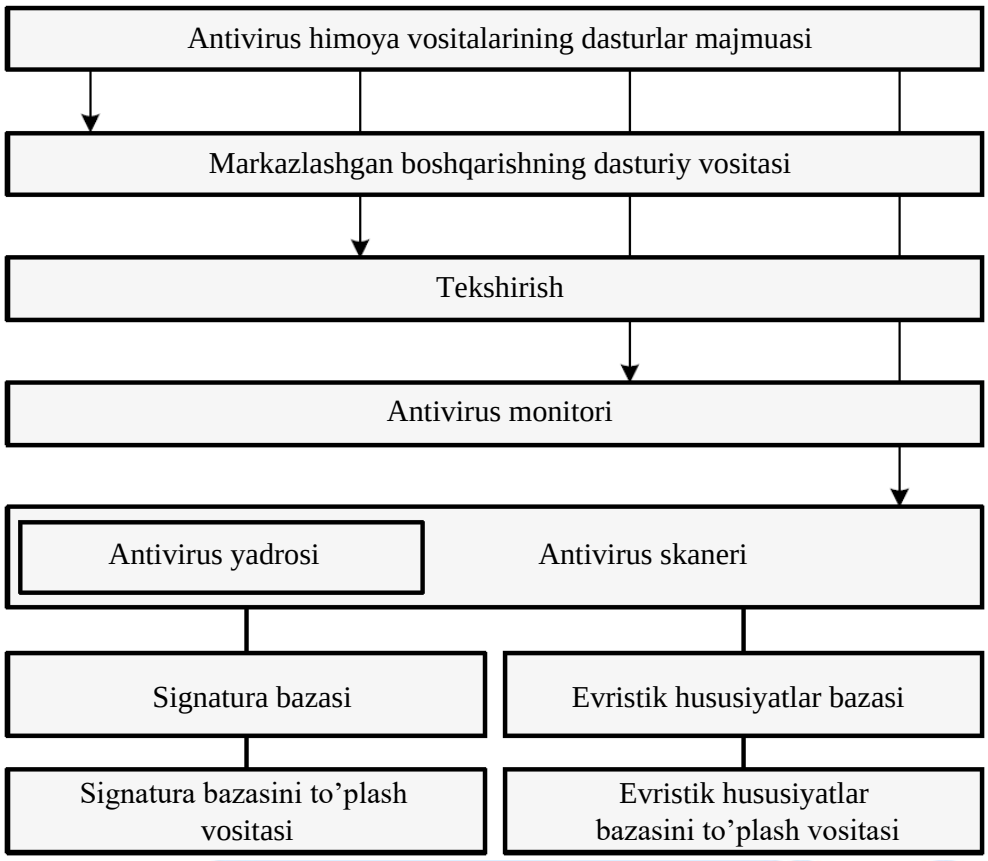


8-rasm. Internet Scanner tizimi misolida himoyalanganlikni tahlillash sxemasi

Viruslardan himoyalash. Yaxshi ishlab chiqilgan zararkunanda dasturni tahlil qilish uchun birinchi qadam bu bir qancha antivirus dasturiy vositalaridan foydalanish kerak bo’ladi, lekin antivirus oeratsion tizimda bo’lsa bu zararkunanda dasturni avtomatik tarzda ko’rib chiqqan bo’ladi. Lekin shuni aytish lozimki, antivirus dasturiy vositalari zararkunanda dasturlarni topishda ideal dastur hisoblanmaydi. Antiviruslar ma’lum shubhali kodlarni shuningdek, gumon qilinuvchi fayllarni aniqlashda evristik

tahlil qiladi va o’zining bazasidan shubhali kodning qismalarini identifikatsiyalashga tayanadi.

Shuni ta'kidlash kerakki, eng qulay detektorlar bir emas, koplab keng tarqalgan viruslarni "ushlaydi". Dastur-fayllar zararlangan dasturlarni tiklashni ta'minlaydi. Ish jarayonida faga virus tanasini "tishlaydi" va virus o'zgartirib yuborgan buyruqlar ketma-ketligini tiklaydi. Biz tilga olayotgan kompyuter viruslari fagasi hozirda yaratilib bo'lingan. Hozir turli fagalarni yig'ish bilan odamlar band bo'lishmoqda. Bu, bizningcha, noto'g'ri. Asosiy e'tiborni zararlanishning oldini olishga qaratish lozim. "1 gramm profilaktika 1 kilogramm davolashga teng" maqoli naqadar to'g'ri.



9-rasm. Antivirus himoya vositalarining dasturlar majmuasi

Ma’lumotlar bazasining serverini himoyalashning usullari juda ko’p va turli bo’lib, ularni bir hususiyat bo’yicha tahlillash murakkab jarayondir. Chunki, har bir usulning o’z vazifasi mavjud. Quyidagi jadvalda himoyalash usullarining vazifalari keltirilgan.

1-jadval. Ma’lumotlar bazasi serverini himoyalash vositalarining tavsifi

Himoyalash usuli	Vazifasi
Shifrlash	Ochiq tarmoqda ma’lumotni qayta akslantirish usullari yordamida ma’nosini o’zgartirish
Sertifikat	Tarmoqqa masofaviy foydalanuvchi yoki xizmatni tanib olish
Trafikni tahlillash	Tarmoqda axborotlar paket ko’rinishida jo’natilib, ularning turi, ya’ni zararli yoki zararsiz va shu tarmoqqa tegishli ekanligini aniqlaydi
Monitoring	Oldindan berilgan qonun-qoidalar asosida tarmoqni kuzatib turadi
Identifikatsiya	Tarmoqqa ulangan foydalanuvchini yozib boradi
Autentifikatsiya	Ruhsatsizn ulanishlarni oldini olish maqsadida, foydalanuvchilarni tanib oladi
Avtorizatsiya	Autentifikatsiyadan o’tgan foydalanuvchining aynan qaysi ma’lumotlar bazasiga ruhsati borligini aniqlab beradi
Ma’murlash	Server va ma’lumotlar bazasiga ulanishlarni boshqarib boradi
IDS/IPS	Ruhsatsiz harakatlarni aniqlash va bartaraf etish
Himoyalanishni tahlillash	Tizimning himoyalanganlik darajasini tahlillaydi
Viruslardan himoyalash	Viruslarni aniqlaydi va ularni bartaraf etadi. Asosan antiviruslardan foydalaniladi

FOYDALANILGAN ADABIYOTLAR RO’YHATI

1. “Davlat sirlarini saqlash to'g'risida”gi O'zbekiston Respublikasining qonuni. 1993 yil, 7 may.

2. ***“Elektron raqamli imzo to'g'risida” gi O'zbekiston Respublikasining qonuni. 2003 yil, 11 dekabr.***

3. ***“Elektron hujjat aylanishi to'g'risida”gi O'zbekiston Respublikasining qonuni. 2004 yil, 29 aprel.***

4. ***Akbarov D. E. “Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi” – Toshkent, 2008 – 394 bet.***

5. ***Ganiev S.K., Karimov M.M., Toshev K.A. Axborot xavfsizligi. 2008.***

6. Information security, Principles and Practice. Mark Stamp. John Wiley & Sons, Inc, 2011.

7. O’zbekiston Respublikasi Prezidentining farmoni. O’zbekiston Respublikasini yanda rivojlantirish bo’yicha Harakatlar strategiyasi to’g’risida. 2017 yil.

8. Newman P. ATM technology for corporate networks //IEEE Communications Magazine. – 1992. – T. 30. – №. 4. – C. 90-101.

9. Ersoy C., Panwar S. S. Topological design of interconnected LAN/MAN networks //IEEE Journal on Selected Areas in Communications. – 1993. – T. 11. – №. 8. – C. 1172-1182.

Internet manbalari:

1. HardTek.ru
2. lifewire.ru
3. fayllar.org
4. iu.edu
5. compress.ru
6. computermaster.ru