O’ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Qo’lyozma huquqida
343.98(075)

DAVLATOVA DILDORA BERDIMUROT QIZI

AXBOROT TIZIMLARI ANOMALIYALARINI SUN’IY IMMUN TIZIMLAR ASOSIDA ANIQLASH MEXANIZM VA ALGORITMLARI

5A330302 – Axborot xavfsizligi mutaxassisligi bo’yicha magistr akademik darajasini olish uchun yozilgan

D I S S E R T A T S I Y A

“Axborot xavfsizligi” kafedra mudiri
“__”_____2022 y.
_____ G’ulomov Sh.R.

Magistratura bo’lim boshlig’i
“__”_____2022 y.
_____ Shakarov Q.A.

Ilmiy rahbar
_____ Ishmurodov A.R.

Toshkent – 2022

O`ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Fakultet: Kiberxavfsizlik
Kafedra: Axborot xavfsizligi
O`quv yili: 2020-2022 yil.

Magistrant: Davlatova D.B.
Ilmiy rahbar: Ishmuratov A.R.
Mutaxassislik: 5A330302-Axborot xavfsizligi

MAGISTRLIK DISSERTATSIYASINING ANNOTATSIYASI

"Axborot tizimlari anomaliyalarini sun'iy immun tizimlar asosida aniqlash mexanizm va algoritmlari" mavzusidagi magistrlik dissertatsiya ishida axborot tizimiga tarmoqdan bo'ladigan tahdidlar, hujumlarni amalga oshirish bosqichlari va aniqlash usullari, suqilib kirishlarni aniqlash va bartaraf etish tizimlari tadqiq va tahlil qilingan. Tahlil natijasiga ko'ra, su'niy immun tizimiga asoslangan anomaliyalarni aniqlash tizimidan foydalanish qulayligi hamda samaradorligi yuqoriligi bilan ajralib turishi aniqlandi. Anomaliyalarni sun'iy immun tizimlar asosida aniqlash mexanizm va algoritmi tadqiq etildi. Sun'iy immun tizimiga asoslangan anomaliyalarni aniqlash tizimini loyihalash amalga oshirilgan.

Kalit so'z: sun'iy immun tizimlar, suqilib kirishlarni aniqlash tizimi, suqilib kirishlarni bartaraf etish tizimi, ma'lumotlar to'plami, NSL-KDD ISCX Dataset, CSIC 2010 Dataset, Enron Dataset.

Ilmiy rahbar: _____
(imzo)

Magistratura talabasi: _____
(imzo)

MINISTRY OF DEVELOPMENT OF INFORMATION TECHNOLOGIES AND COMMUNICATIONS OF THE REPUBLIC OF UZBEKISTAN

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES NAMED AFTER MUHAMMAD AL-KHWARIZMI

Faculty: Cybersecurity
Department: Information Security
Academic year: 2020-2022 y.

Master: Davlatova D.B.
Supervisor: Ishmuratov A.R.
Direction: 5A330302- Information Security

ABSTRACT OF MASTER'S DISSERTATION

In the master's dissertation on "Mechanisms and algorithms of anomaly detection of information systems based on artificial immune systems" the network threats to the information system, stages and methods of attack detection, intrusion detection and prevention systems are considered and analyzed. Based on the results of the analysis, it was found that the anomaly detection system based on artificial immune system is easy to use and highly effective. The mechanism and algorithm for detecting anomalies based on artificial immune systems are considered. An anomaly detection system based on an artificial immune system has been developed.

Key words: artificial immune system, intrusion detection system, prevention detection system, dataset, NSL-KDD ISCX Dataset, CSIC 2010 Dataset, Enron Dataset.

The scientific leader: _____
(signature)

Master's student: _____
(signature)

MUNADIJA

KIRISH

O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi “2022-2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi PF 60-sonli farmoni bilan tasdiqlangan “2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi”da fuqarolarning axborot olish va tarqatish erkinligi borasidagi huquqlarini yanada mustahkamlash borasida bir qator vazifalar, jumladan, shaxsiy va sir saqlanishi lozim bo‘lgan ma’lumotlarni Internet tarmog‘ida oshkor qilish bilan bog‘liq daxlsizlik huquqi buzilishining oldini olish va kiberjinoyatchilikning oldini olish tizimini yaratish vazifalari qo‘yilgan [1].

Bundan tashqari 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya asosida Qonunchilik palatasi tomonidan 2022-yil 25-fevralda qabul qilingan va Senat tomonidan 2022-yil 17-martda ma’qullangan “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqildi. Ushbu qonun rasman kuchga kirmagan bo‘lsa ham (Kuchga kirish sanasi 17.07.2022) qonunning asosiy maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat. Mazkur qonunda kiberjinoyatlarning oldini olish, aniqlash va bartaraf etish bo‘yicha barcha zarur choralarni ko‘rish alohida ta’kidlab o‘tilgan [2]. Yuqorida qayd etilgan hamda mazkur faoliyatga tegishli boshqa me’yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya tadqiqoti ma’lum darajada xizmat qiladi.

Magistrlik dissertatsiya mavzusining asoslanishi va uning dolzarbligi. Axborot tizimida saqlanadigan, qayta ishlanadigan va telekommunikatsiya tarmog‘i orqali uzatiladigan axborot hajmining ortishi o‘z navbatida xavfsizlik ta’minlash tizimidagi tahdid va zaifliklar sonini ortishiga sabab bo‘lmoqda. Tarmoq hujumlarini aniqlash bugungi kunda tarmoq texnologiyalarining eng dolzarb muammolaridan biri hisoblanadi. Tamoqda trafikni filtrlash mexanizmlari tarmoq xavfsizligini ta’minlashning muhim usulidir. Bugungi kunda tarmoqdan bo‘ladigan tahdidlardan himoyalanish muhim masalalardan biri bo‘lib qolmoqda. Antivirus dasturlari, tarmoqlararo ekran texnologiyalari, suqilib kirishlarni aniqlash

va ularni bartaraf etish, hamda xavfsizlik holatini skanerlarini tizimlarini ishlab chiqishdagi yangi yondashuvlar himoyalash tizimlarini umumiy holatini tubdan o‘zgartirmaydi.

Tashqi tarmoqdan keluvchi so‘rovlardagi anomal holatlarni aniqlash tizimlarining mexanizm va algoritmlarini takomillashtirish, ularni OSI modeli sathlarida ishlash unumdorligini oshirish, filtrlash qoidalarini hamda intellektual tizimlar uchun ma’lumotlar to‘plamini shakllantirish usullarini ishlab chiqish muhim ahamiyat kasb etmoqda. Bu borada olib borilayotgan ilmiy-tadqiqot ishlarida quyidagi jihatlarga alohida e’tibor qaratilmoqda: kompyuter tarmoqlarini ishonchli himoyasini ta’minlash maqsadida resurslarning ma’lum kategoriyalaridan foydalanishni cheklovchi usullarni ishlab chiqish; ikki qatlamli rekurrent neyron tarmoq asosida kiruvchi trafikni filtrlash usullari va dasturiy majmualarini ishlab chiqish; ma’lumotlarni sun’iy intellekt usullari asosida filtrlash modellarini yaratish.

Tarmoq trafigini tasniflash jarayonida dolzarb muammolardan biri anomal so‘rovlarni aniqlash hisoblanadi, ushbu masalalarni hal qilishda mashinali o’qitishga asoslangan anomaliyalarni aniqlash tizimlari yuqori samaradorlikni ko‘rsatmoqda. Yangi qo’llanilayotgan usullar va texnologiyalarni ishonchliligi va samaradorligi, hamda ularni real vaqt rejimida amalga oshirish bilan bog’liq masalalar noaniq bo’lib qolmoqda, mashinali o‘qitish texnologiyasiga asoslangan istiqbolli yo’nalishlardan biri sun’iy immun tizimlarini qo‘llagan holda suqilib kirishlarni aniqlash tizimini ishlab chiqish dolzarb hisoblanadi.

Tadqiqot obyekti va predmeti. Axborot tizimi lokal tarmog‘iga internet muhitidan kelayotgan tashqi so‘rovlarda anomaliyalarni aniqlash jarayonini tadqiqotning ob’yekti sifatida keltirish mumkin.

Tadqiqot predmeti sifatida tarmoq trafigida anomaliyalarni sun’iy immun tizimlar asosida aniqlash mexanizmi va algoritmlarini olish mumkin.

Tadqiqot maqsadi va vazifalari. Magistrlik dissertatsiya ishini bajarishdan maqsad axborot tizimlariga tarmoqdan kelayotgan so’rovlardagi anomaliyalarni su’niy immun tizimlar asosida aniqlash mexanizm va algoritmlari samaradorligini

oshirishdir.

Ushbu maqsadga erishish uchun tadqiqot ishini bajarishda quyidagi vazifalar belgilab olindi:

- axborot tizimlariga bo‘ladigan tahdidlarni tavsiflash va tasniflash;
- hujumlarni amalga oshirish bosqichlari va aniqlash usullarini, suqilib kirishlarni aniqlash hamda bartaraf etish tizimlarini tahlil qilish;
- anomal so‘rovlarni aniqlashda qo‘llaniladigan ma’lumotlar to‘plamini tahlil qilish;
- sun’iy immun tizimiga qo‘yiladigan talablarni va uning elementlarini tadqiq qilish;
- su’niy immun tizimiga asoslangan anomaliyalarni aniqlash tizimi arxitekturasini loyihalash;
- mashinali o‘qitishga asoslangan anomaliyalarni aniqlash tizimi samaradorligini tahlil qilish;
- sun’iy immun tizimiga asoslangan anomaliyalarni aniqlash tizimini loyihalashni amalga oshirish.

Ilmiy yangiligi:

- sun’iy immun tizimiga asoslangan anomal so‘rovlarni aniqlash tizimi arxitekturasi loyihalashtirildi;
- sun’iy immun tizimiga asoslangan anomaliyalarni aniqlash tizimi loyihalashtirildi va samaradorligi baholandi.

Tadqiqotning asosiy masalalari va farazlari. Axborot tizimlarida tarmoqdan keluvchi so‘rovlarda anomaliyalarni aniqlash tarmoq xavfsizligi muammolarini minimallashtirishga va tarmoq trafigidagi zaifliklarni oldini olishga imkon yaratib beradi.

Tadqiqot mavzusi bo‘yicha adabiyotlar tahlili. Mazkur mavzu doirasida chet el va resublikamiz olimlari va professorlari ilmiy izlanish ishlarini olib borganlar va tezis, ilmiy maqolalar hamda bir qancha kitob nashrlarida o‘z tajribalarini keltirib o‘tishgan.

Bularga misol sifatida: L.Anderson “Computer security threat monitoring and surveillance”, D.Allen “The Role of Intrusion Detection Systems”, D.Anderson “Next-generation Intrusion Detection Expert System (HIDES)”, D. Denning “An intrusion detection model”, D.Protic “Intrusion detection based on the artificial immune system”; LinY-D., LuCh-N., LaiY- Ch. “Application classification using packet size distribution and port association”; V.Vasilyev. “Интеллектуальные системы защиты информации”; Gulomov Sh.R., Abdurakhmanov A.A., Nasrullaev N.B. “Design Method and Monitoring Special Traffic Filtering under Developing” kabi nashrlarni keltirib o‘tishimiz mumkin.

Tadqiqotda qo‘llanilgan metodikaning tavsifi. Dissertatsiya ishini olib borish jarayonida ehtimollar nazariyasi, matematik statistika, obrazlarni tanib olish nazariyasi, sun’iy neyron tarmoq nazariyasi va noaniq mantiq, matematik modellash usullari, qiyosiy tahlillash va baholash usullaridan foydalanilgan.

Tadqiqot natijalarining nazariy va amaliy ahamiyati. Ishlab chiqilgan sun’iy immun tizimiga asoslangan anomal so‘rovlarni aniqlash tizimini suqilib kirishlarni aniqlash tizimlarini loyihalashda qo’llash imkoniyati bilan nazariy ahamiyat kasb etadi.

Magistrlik dissertatsiya ishining amaliy ahamiyati taklif etilgan sun’iy immun tizimiga asoslangan anomal so‘rovlarni aniqlashning mexanizm va algoritmi tarmoq anomaliyalarni aniqlash qobiliyatini qiyosiy baholash imkonini beradi.

Ish tuzilmasining tavsifi. Ushbu tadqiqot ishi: kirish, 3 ta bob, xulosa va foydalanilgan adabiyotlar ro‘yxatidan iborat.

Ushbu tadqiqot ishi 20 ta jadval, 7 ta rasmdan iborat. Ilmiy tadqiqot ishining umumiy hajmi 69 sahifani tashkil etadi.

1 BOB. AXBOROT TIZIMLARIDA MAVJUD XAVF-XATARLAR TAHLILI

1.1 Axborot tizimlariga bo‘ladigan tahdidlar tasnifi

Maxfiylikni buzish tahdidlari maxfiy ma’lumotlarni olishga (o‘g‘irlashga) qaratilgan. Ushbu tahdidlar amalga oshirilganda, ma’lumotlarga kirish huquqiga ega bo‘lmagan shaxslarga ma’lum bo‘ladi. Axborot tizimida saqlanadigan yoki ma’lumotlarni uzatish kanallari (tarmoqlari) orqali uzatiladigan ma’lumotlarga ruxsatsiz kirish, ushbu ma’lumotlarni nusxalash axborotning maxfiyligini buzish hisoblanadi.

Axborot tizimida saqlanadigan yoki ma’lumotlarni uzatish tarmog‘i orqali uzatiladigan axborotning yaxlitligini buzish tahdidlari ma’lumotlarni o‘zgartirish yoki buzishga qaratilgan bo‘lib, axborot mazmunini buzilishiga yoki to‘liq yo‘q qilinishiga olib keladi. Axborotning yaxlitligi buzg‘unchi tomonidan atayin, shuningdek, tizimni o‘rab turgan tashqi muhitning obyektiv ta’siri (aralashuvi) natijasida buzilishi mumkin. Bu tahdid, ayniqsa, axborot uzatish tizimlari - kompyuter tarmoqlari va telekommunikatsiya tizimlari uchun dolzarbdir. Axborotning yaxlitligini qasddan buzish, avtorizatsiyalangan foydalanuvchilar tomonidan qonuniy amalga oshiriladigan ruxsat etilgan o‘zgartirish bilan chalkashtirmaslik kerak.

Tizimning foydalanuvchanligini buzish tahdidlari (xizmat ko‘rsatishdan voz kechish) muayyan harakatlar axborot tizimining ishlash qobiliyatini pasaytiradigan yoki uning ba’zi resurslaridan foydalanishni blokirovka qiladigan vaziyatlarni yaratishga qaratilgan. Axborot tizimlari xavfsizligiga tahdidlar bir necha mezonlarga ko‘ra tasniflanadi.

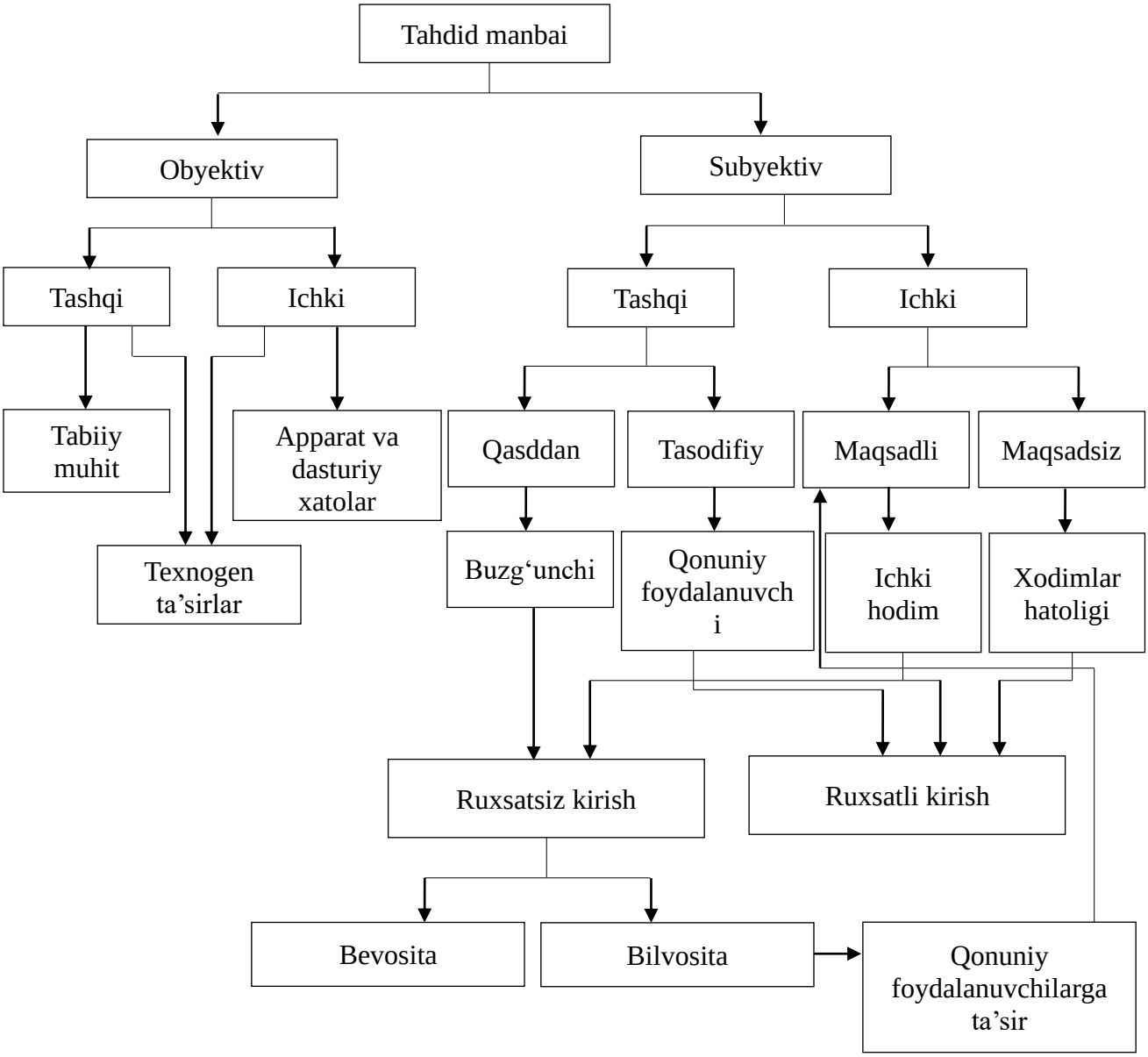
Tasodifiy taxdidlarning sabablari:

- tabiiy ofatlar va elektr ta’minotidagi uzilishlar natijasida yuzaga kelgan favqulodda vaziyatlar;

- dasturiy ta’minotdagi xatolar;

- xizmat ko’rsatuvchi xodimlar va foydalanuvchilarning ishidagi xatolar;

- tashqi muhit ta’sirida, shuningdek tizimdagi zich trafik tufayli aloqa liniyasidagi shovqin (simsiz tarmoqlar uchun hos).



1.1-rasm. Axborot resurslariga bo‘ladigan tahdidlar tasnifi

Qasddan amalga oshiriladigan taxdidlar buzg‘unchi maqsadli harakatlari bilan bog‘liq bo‘lib, u har qanday manfaatdor shaxs (raqobatchi, tashrif buyuruvchi, xodimlar va boshqalar) bo‘lishi mumkin. Hujumchining harakatlari maqsadga qarab turli bo‘lishi mumkin: xodimning o‘z martabasidan noroziligi, moddiy manfaatdorligi, qiziquvchanligi, raqobati, har qanday holatda ham o‘zini ko‘rsatish istagi va boshqalar.

Ichki tahdidlar maxfiy ma’lumotlarni saqlovchi tizimda o‘rnatilgan ob’yekt xodimlari tomonidan amalga oshiriladi. Bunday tahdidlarning paydo bo‘lishining

sabablari jamoadagi nosog‘lom muhit yoki ba’zi xodimlar tomonidan bajarilgan ishlardan norozi bo‘lishi mumkin, ular ma’lumot olishdan manfaatdor shaxslarga ma’lumot berish uchun harakatlarni amalga oshirishlari mumkin.

Tashqi tahdidlar deganda uchinchi shaxslar tomonidan yaratilgan va tashqi muhitdan kelib chiqadigan tahdidlar tushuniladi, masalan:

- axborotni buzish, yo‘q qilish, o‘g‘irlash yoki korxona axborot tizimlariga xizmat ko‘rsatishdan voz kechishga olib keladigan tashqi tarmoqdan (masalan, Internet) hujumlar;

- zararli dasturlarni tarqatish;

- nomaqbul tarqatmalar (spam);

- axborot tizimlarida elektromagnit energiyani induksiya qilish uchun elektromagnit maydon manbasidan foydalangan holda, ushbu tizimlarning apparat va dasturiy ta’minotining normal ishlashini (noto‘g‘ri ishlashini) buzilishiga olib keladigan darajadagi axborotga ta’sir qilish;

- radioqabul qiluvchi qurilmalar yordamida axborotni ushlash;

- muhandislik tarmoqlaridan ruxsatsiz foydalanish orqali ma’lumotlarga ta’sir qilish;

- maxfiy ma’lumotlarni olish uchun korxona xodimlariga ta’sir qilish.

Tizimni buzishga bo‘ladigan harakatlar xavflilik darajasiga ko‘ra: zaiflik, tahdid va hujumga olib keluvchilarga bo‘lish mumkin.

Zaiflik – bu tizimda mavjud bo‘lgan xavfsizlik muammosi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi. Zaifliklar tizimlarda katta yoki kichik tarzda mavjud bo‘ladi.

Tahdid – bu mavjud bo‘lgan zaiflik natijasida bo‘lishi mumkin bo‘lgan hujum turi bo‘lib, ular asosan tizimning kamchiliklarini o‘rganish natijasida kelib chiqadi.

Hujum – bu mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi.

Axborot tizimlari komponentlariga nisbatan quyidagi xavf-hatarlar mavjud, ya’ni uzilish, tutib qolish, o‘zgartirish va soxtalashtirish:

- *uzilish* - qandaydir tashqi harakatlar (ishlar, jarayonlar)ni bajarish uchun hozirgi ishlarni vaqtincha markaziy protsessor qurilmasi yordamida to‘xtatishdir, ularni bajargandan so‘ng protsessor oldingi holatga qaytadi va to‘xtatib qo‘yilgan ishni davom ettiradi. Protsessorlar ikki turdagi uzilishlar bilan ishlashni vujudga keltirishi mumkin: dasturiy va texnik.

- *tutib qolish* - jarayon oqibatida buzg‘unchi dasturiy vositalar va axborotlarning turli axborot tashuvchilarga kirish huquqini qo‘lga kiritadi.

- *o‘zgartirish* - ushbu jarayonda buzg‘unchi nafaqat kompyuter tizimi komponentlariga (ma’lumotlar to‘plamlari, dasturlar, texnik elementlari) kirishni qo‘lga kiritadi, balki ular bilan manipulyatsiya (o‘zgartirish, ko‘rinishini o‘zgartirish) ham qiladi.

- *soxtalashtirish* – ushbu jarayon yordamida buzg‘unchi tizimda hisobga olinmagan vaziyatlarni o‘rganib, undagi kamchiliklarni aniqlab, keyinchalik o‘ziga kerakli harakatlarni bajarish maqsadida tizimga qandaydir soxta jarayonni yoki tizim va boshqa foydalanuvchilarga soxta yozuvlarni yuboradi.

Xakerlik xujumi - masofadagi xisoblash mashinasi ustidan nazoratni qo‘lga olish (xuquqlarni oshirish) maqsadidagi xarakat yoki xizmat ko‘rsatishdan voz kechishga olib kelish.

Crack – dasturiy vositalarni buzishga imkon beruvchi dastur. Umuman olganda crack ham bu buzish usulining bir turi.

Patch (patch) – kompyuter fayllariga avtomat ravishda belgilangan o‘zgartirishlarni kiritish uchun mo‘ljalangan axborot.

Troyan otlari bu, dastur qonuniy ko‘rinuvchi lekin ishga tushgandan so‘ng noqonuniy xarakatlarni amalga oshiradi. Ular parollar saqlanuvchi joyni aniqlash, tizimga kirishni amalga oshirish uchun xavfsizligini kamaytirish yoki qattiq diskdagi dasturni, ma’lumotlarni o‘chirish uchun foydalanilishi mumkin. Troyan otlari virusga o‘hshaydi, lekin fayllarni zararlash orqali ko‘paya olmaydi, masofadan turib kompyuter ustidan boshqaruvga imkon beradi [3].

DoS va DDoS- hujumlari tarmoqqa yo‘naltirilgan, ular qo‘shimcha so‘rovlar bilan to‘ldirib tashlaydi, buning natijasida foydali trafik kamayadi yoki uzilib

qoladi. Bazaga zarar yetkazuvchi viruslar va chuvalchanglardan farqli ravishda DoS –hujumlari tarmoq ishini ma’lum vaqtga buzib qo‘yadi, DDoS-hujumlari zararlangan tarmoq kompyuterlaridan foydalanadi. “Zombi”, rolini bajaruvchi kompyuterlar soxta xatlar yuboradi shu bilan sohta trafikni oshiradi. Bu hujum turi boshqa hujumlarga o‘xshamaydi. Unda tarmoqdan foydalanish uchun ruxsat olish yoki qandaydir axborotni qo‘lga kiritish o‘rniga, qonuniy foydalanuvchilar ushbu tizim, ilova yoki operatsion tizimdan foydalana olishlarini to‘sishni maqsad qiladi yoki ularni foydalanuvchanlik darajasini yo‘qotishga harakat qiladi. Natijada qonuniy foydalanuvchi tizim resursidan foydalana olmaydi.

Tinglash. Kompyuter tarmoqlarida uzatilayotgan ma’lumotlarning asosiy hajmi ochiq holda uzatilganligi sababli, tahdidchiga bu ma’lumotlarni tinglash va tahlil qilish imkonini yaratadi. Kompyuter tarmog‘ini tinglash uchun mahsus *sniffer* deb nomlanuvchi dasturlar talab etiladi. Sniffer dasturlari amaliy sathda ishlab, ma’lum domenda uzatilayotgan barcha paketlarni tutib qolish imkoniyatini yaratadi.

*Ma’lumotlarni o‘zgartirish.*Ko‘p hollarda tahdidchi faqat tarmoqdagi ma’lumotlarni tinglash bilan chegaralanmaydi. Ko‘p hollarda tahdidchi yuboriladigan paketlarni o‘zgartirishga urinib ko‘radi va buning uddasidan chiqadi ham. Bu hol hattoki yuboruvchining ismi noma’lum bo‘lganda ham amalga oshiriladi. Umuman aytganda tahdidchi tomonidan asosiy maqsad qilib ma’lumotni butunligini buzish hisoblanadi.

*Tarmoq trafigini tahlil qilish.*Bu tahdid usuli tarmoqni tinglash davomida amalga oshirilib, paketlarni tahlil qilish orqali tarmoq topologiyasi, arxitekturasi, kritik ma’lumotlarni (masalan, ochiq holda uzatilganda foydalanuvchi kredit karta raqami yoki parol) bilishga harakat qiladi. Bu tahdid ko‘p holda FTP va Telnet protokollariga qaratiladi.

Ishonchli sub’yektni almashtirish. Ko‘plab tarmoqda va operatsion tizimlarda kompyuterni tanitish uchun IP - manzillardan foydalaniladi. Ko‘p hollarda qabul qiluvchiga bu manzillarni noqonuniy ravishda o‘zgartirish hollari

kuzatiladi va bu ko‘rinishdagi tahdid turi *manzilni soxlashtirish* yoki *IP - spoofing* deb ataladi.

Bu turdagi tahdid IP - manzilga asoslangan autentifikatsiyalashga katta ziyon yetkazishi mumkin. Bu holda boshqa turdagi autentifikatsiyalash usulidan yoki ikkinchi faktor asosida autentifikatsiyalashdan foydalanish zarur bo‘ladi.

Vositachilik. Bu tahdid ma’lumotlarni aktiv eshitishni, tutib olishni va boshqarishni ko‘zda tutib, nomalum uzel tomonidan amalga oshiriladi. Ko‘plab past darajadagi tarmoq sathlarida, uzatuvchi tomon kim bilan ma’lumot almashayotganini aniq bilmaydi va ko‘p hollarda bu tahdidga duch kelishadi.

*Shifrlanmagan kalitlarni almashinishda vositachilik (man-in-the-middle, MITM).*Bu tahdidni amalga oshirish uchun o‘rtaga turgan tahdidchi uchun uzatiladigan paketlarga ruxsat bo‘lishi zarur. Bu turdagi tahdidni amalga oshirishda odatda sniffer dasturlaridan, transport protokollari va marshrutlash protokolidan foydalaniladi.

Seansni tutib qolish (seans hijacting). Ulanishdagi pochta serveri bilan, dastlabki autentifikatsiyadan so‘ng, qonuniy foydalanuvchi tahdidchi “yordami bilan” boshqa yangi hostga ulanadi. Dastlabki server esa ulanishni uzadi. Natijada qonuniy foydalanuvchining “suhbatdoshi” bilinmas tarzda almashtiriladi. Bu holda tahdidchi quyidagi imkoniyatlarga ega bo‘lishi mumkin:

- noto‘g‘ri ma’lumotlarni yoki xizmatlarni ko‘rsatish orqali avariyali xolatga olib kelish;
- kompyuterni yoki butun tarmoqni to‘ldirish;
- trafikni blokirovkalash orqali qonuniy foydalanuvchini tizim resursidan foydalanishga to‘sqinlik qilish.

*Parolga qaratilgan hujumlar.*Bu hujumning asosiy maqsadi - foydalanuvchining login va parolini qo‘lga kiritishga qaratilgan. Buni amalga oshirishda quyidagi turdagi hujumlardan foydalaniladi.

Internet tarmog‘ida, u yoki bu funksiyani amalga oshiradigan turli ilovalar o‘rtasida manzilni aniqlash va tashish vositasi sifatida TCP/IP stekidan foydalanadigan protokollar soni ortib bormoqda. Ba’zi protokollar global tarmoqda

standart, ba’zilari faqat eksperimental ishlanmalar hisoblanadi. Protokollarning har biri yetti qatlamli OSI modelining o‘z qatlamida ishlaydi.

1.1 – jadval.

OSI modeli qatlamlari bo‘yicha protokollar

OSI sathi	OSI qatlamiga mos keladigan protokollar
Ilova	*BGP, DNS, FTP, HTTP, HTTPS, IMAP, LDAP, POP3, SNMP, SMTP, SSH, Telnet, XMPP*
Seans/taqdimot	*SSL, TLS*
Transport	*TCP, UDP, ICMP*

Tarmoqdagi har bir protokol turli xil tizimlarning bir-biri bilan o‘zaro aloqasi uchun javob beradi, afzalik va kamchilik tomonlarini o‘z ichiga oladi. Amalga oshirishdagi har qanday bo‘shliq maxfiylik, foydalanuvchanlik va ma’lumotlar yaxlitligi nuqtai nazaridan potentsial xavf tug‘diradi. Tizimlar bir-biri bilan chambarchas bog‘langan bo‘lishi, himoyalangan komponentlarga nisbatan ham tahdidlarning amalga oshirish ehtimoli saqlanib qoladi. Masalan, veb-serverning ishlashi doirasida kiruvchi parametrlarni noto‘g‘ri shakllantirilishi ushbu veb-server ishlayotgan operatsion tizimning beqarorligiga olib kelishi mumkin. Hozirgi kunda Internetning asosiy transport protokollari TCP va UDP hisoblanadi.

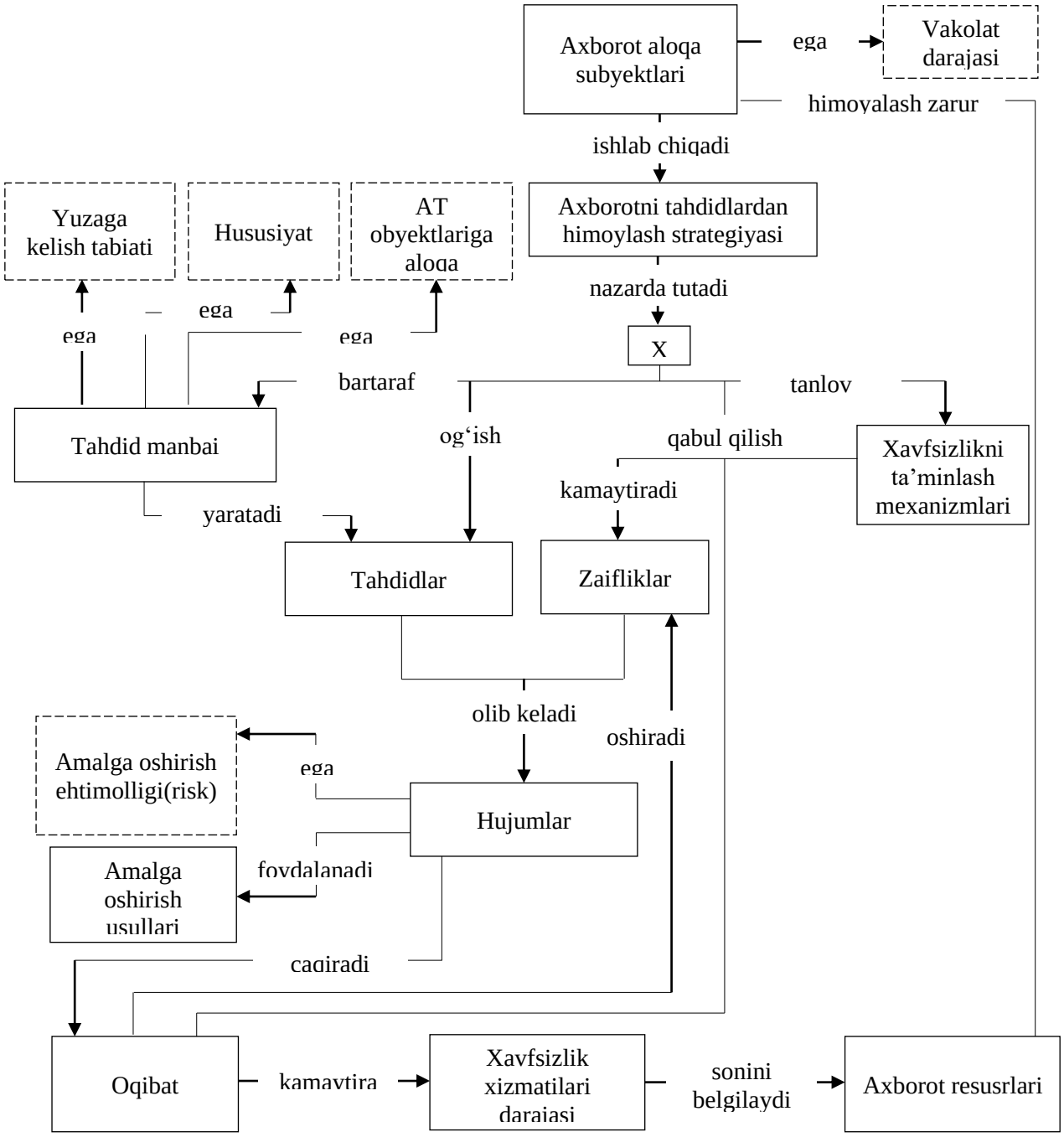
TCP, UDP va ICMP steklarida, umuman olganda, tahdidlarning 4 ta katta sinfi ajralib turadi:

Xizmat ko‘rsatishdan voz kechish (Denial of Service, DoS). Buzg‘unchi tizimning qonuniy (ruxsat etilgan) foydalanuvchilariga taqdim etilgan tizim resurslariga (serverlariga) kira olmaydigan yoki kirishni qiyinlashtiradigan sharoitlarni yaratadigan tahdidlar sinfi.

Masofadagi infratuzilmaga hujum (Remote to Local, R2L). Jabrlanuvchining infratuzilmasiga kirish huquqiga ega bo‘lmagan buzg‘unchi kirish tizimini buzish orqali uni olishga harakat qiladigan tahdidlar sinfi.

Imtiyozlarni oshirish (User to Root, U2R). Buzg‘unchi uchun jabrlanuvchining infratuzilmasiga kirish huquqi cheklangan, muhim operatsiyalarni boshqarish va bajarish uchun ma’muriy huquqlarni olishga harakat qiladigan tahdidlar sinfi.

Skanerlash (Probe). Buzg‘unchi hujum qilinadigan tizim haqida har qanday ma’lumot olishga harakat qiladigan tahdidlar sinfi [4].



1.2-rasm. Axborot tizimlari xavfsizligini ta’minlash tuzilmasi

1.2 Hujumlarni amalga oshirish bosqichlari va aniqlash usullari

Axborot tizimini global tarmoq bilan o‘zaro aloqasi doirasida tahdidni amalga oshirishning muhim qismi bu hujum (suqilib kirish). Axborot tizimiga hujum (suqilib kirish) - buzg‘unchining axborotni uchta asosiy xususiyatidan biri – bo‘lgan foydalanuvchanlik, yaxlitlik va maxfiylikni buzishga qaratilgan qasddan harakatlari majmuidir. Tarmoq hujumlarini aniqlash va axborot tizimlariga kompyuter hujumlarining belgilarini aniqlash tizimlari uzoq vaqtdan beri axborot tizimlarini himoya qilishning zarur bosqichlaridan biri hisoblanadi.

Hujumchilarning ko‘pchiligi tizimni suqilib kirishni amalga oshirish bo‘yicha mutaxassis bo‘ladi, kompyuter tarmoqlariga ruxsatsiz kirish usullari va dasturlarni yaratishadi, avtomatlashtirilgan vositalardan kamdan-kam hollarda foydalanishadi. Hozir, bu sohada bilimi past bo‘lgan “xavaskor” lar soni ko‘p, ular suqilib kirishni amalga oshiruvchi avtomatlashtirilgan vositalarni va eksploytlarni (exploit-zararkunanda kod, dasturiy ta’minotning ma’lum xatolardan va buzg‘unchining apparat-dasturiy komplekslarning normal ishlashini buzishda qo‘llaniladigan usullardan foydalanadi) ishlatadilar. Boshqa so‘zlar bilan aytganda, avtomatik hujum vositalarini takomillashishi bilan bir qatorda buzg‘unchilar bilim darajasi va malakasining pasayib ketishidir.

Endi hujumlar bir necha sekund davom etadi va sezilarli zarar yetkazishi mumkin. Misol uchun, “xizmatdan voz kechish” hujumi web-magazinlar yoki onlayn-birjalarni uzoq vaqtga ishdan chiqarib qo‘yishi mumkin. Bunday hujumlar keng tarqalgan hisoblanadi va ulardan himoyalanish yuqori tezlikda rivojlanmoqda.

Hujumlarning turlari bo‘yicha tasnifi. Hujumlarning faol va passiv turlari mavjud. Faol hujumlar ta’sirining natijasi axborot tizimining buzilishi bo‘lsa, passiv hujumlar esa tizimdan uning ishlashini buzmasdan ma’lumot olishga qaratilgan. Umuman olganda, hujumchi tomonidan tahdidni amalga oshirish quyidagi bosqichlardan iborat:

Razvedka qilish bosqichi. Ushbu bosqichda hujumchi hujum obyekti haqida iloji boricha ko‘proq ma’lumot olishga harakat qiladi (Probe so‘rovlari), buning

asosida tahdidlarni amalga oshirishning keyingi bosqichlarini rejalashtirish amalga oshiriladi. Hujum tizimi va uning parametrlari haqida ma’lumot yig‘ish. Bunday ma’lumotlar: ishlatiladigan veb-server OT yoki ma’lumotlar bazasining turi va versiyasi, ma’lumotlarni uzatish protokolining o‘ziga xos xususiyatlari va boshqalar. Qo‘shimcha tahdid vektori - dasturiy ta’minotni onlayn yangilashning yo‘qligi.

Amalga oshirish imkoniyatini o‘rganish. Ushbu bosqichda hujumchi belgilangan tahdidni keyinchalik amalga oshirishni hisobga olgan holda tarmoq infratuzilmasini tekshiradi, aniqlangan zaifliklardan foydalanish imkoniyatini o‘rganadi. Tarmoq infratuzilmasi sohalarini tahlil qilish quyidagilarni o'z ichiga oladi: Internet - provayderning server maydoni yoki hujum qilinadigan kompaniyaning uzoq ofis tugunlari. Vakolatli foydalanuvchilarning manzillarini, tizim axborot resurslarining egalarini, vakolatli jarayonlarini va boshqalarni aniqlaydi. Bunday xatti - harakatlarni aniqlash juda qiyin, chunki ular himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash tizimlari va boshqalar) ta’sir doirasidan tashqi maydonda amalga oshiriladi.

Skanerlash. Xizmatlarni aniqlash (xizmatni aniqlash), odatda, ochiq portlarni aniqlash (portni skanerlash) orqali amalga oshiriladi. Bunday portlar ko‘pincha TCP yoki UDP protokollariga asoslangan tizim xizmati bilan bog‘liq. Operatsion tizimni aniqlash. (OS detection) - turli xil operatsion tizimlarda turli TCP/IP-Stack dasturlarini hisobga olgan holda so‘rovlarga javoblarni tahlil qilish.

Suqilib kirish bosqichi. Ushbu bosqichda hujumchi hujum qilinayotgan tugunlarning resurslariga ruxsatsiz kirish huquqini qo‘lga kiritadi (R2L). Perimetrni himoya qilish vositalarini yengib o‘tishni nazarda tutadi

Axborot tizimiga hujum qilish bosqichi. Tahdidning ushbu bosqichi hujumchi tomonidan belgilangan maqsadlariga erishishga qaratilgan. Bunday xatti-harakatlarga misol qilib, AT ishlash qobiliyatini ishdan chiqarish, tizimda saqlanadigan maxfiy ma’lumotlarga kirish, ma’lumotlarni o‘chirish yoki o‘zgartirish va boshqalar bo‘lishi mumkin. Bunday holda, hujumchi AT da izlarni o‘chirishga qaratilgan harakatlarni ham bajarishi mumkin (U2R, DoS).

Hujumning keyingi rivojlanish bosqichi. Ushbu bosqichda AT ning boshqa ob’yektlariga hujumni davom ettirish uchun zarur bo‘lgan harakatlar amalga oshiriladi. Hujumni yakunlash bosqichi tajovuzkor tomonidan ruxsatsiz harakatlarni yashirishdir [4].

Shunday qilib, tahdidlarni amalga oshirish aniq tuzilishga ega, bu esa uni amalga oshirishning har bir bosqichini aniq aniqlash imkonini beradi.

Bugungi kunga kelib, tizimlar o‘rtasida uzatiladigan xavfli, anomal so‘rovlarni aniqlashga imkon beruvchi ko‘plab usullar mavjud. Umumiy holatda ularni aniqlash uchun signaturali va signaturasiz usullar qo‘llaniladi. Ushbu usullarning har biri o‘zining afzallik va kamchiliklariga ega.

Hujumlarning ko‘p turlari mavjud va ularni xavflilik darajasi bo‘yicha farqlash mumkin:

- parollarni aniqlash;
- replikatsiya kodlar;
- parollarni buzish;
- ma’lum zaifliklardan foydalanish;
- audit tizimlarini o‘chirish/aylanib o‘tish;
- ma’lumotlar o‘g‘rilash;
- backdoors (dasturga maxsus kirish yo‘llari–dasturchi tomonidan tashlab ketilgan yoki dasturni yozish jarayonidagi xatoliklar bilan bog‘liq);
- snifferlardan foydalanish (nazorat tizimlari);
- zarur ma’lumotlarni olish uchun tarmoqni diagnostika qilish dasturlaridan foydalanish;
- zaifliklarni aniqlovchi avtomatlashtirilgan skanerlardan foydalanish;
- IP-paketlardagi ma’lumotlarni almashtirish;
- xizmat qilishdan voz kechish (DOS) hujumlar;
- web-serverlarga hujum (skriptlar);
- yashirin skanerlash texnologiyasi;
- taqsimlangan hujum vositalari.

Signaturaga asoslangan usullari. Signaturali usullarning afzalliklari quyidagilardan iborat:

- signaturalar bazasida mavjud so‘rovlarni (yoki ularning shablonlarini) yuqori tezlikda aniqlash imkoniyati;
- noto‘g‘ri ishga tushishlarning past darajasi, chunki signaturalar bazasiga faqat anomal faollik haqidagi ma’lumotlar kiritilgan.

Ushbu yondashuvning kamchiliklari:

- yangi turdagi xavfli so‘rovlarni aniqlashning imkoni yo‘qligi, paydo bo‘lish (masalan, eksploit yoki ineksiya shaklida (nolinchi darajadagi tahdid)) va signatura bazasini chiqarilishi o‘rtasidagi vaqt oralig‘i mavjud, so‘nggi tugunlar zaif bo'lib qoladi;
- tahdid signatura bazasini doimiy va tezkor yangilash zarurati;
- so‘rov obyektining nusxasini qo‘lda yaratish bilan signatura yaratishning ko‘p vaqt talab qiladigan jarayoni. Signaturaga asoslangan usulning ishlashiga misol sifatida DPI texnologiyasini keltirish mumkin (Deep Packet Inspection);
- statistik ma’lumotlarni to‘plash, tarmoq paketlarini tarkibi bo‘yicha tekshirish va filtrlash texnologiyasidir.

1.3 Suqilib kirishlarni aniqlash va bartaraf etish tizimlari

Axborot tizimlariga xujum, tizimning zaifliklaridan foydalanib, qayta ishlanayotgan axborotning butunligi, maxfiyligi, foydalanuvchanligini buzilishiga olib keluvchi taxdidchining ataylab qilgan harakatlardir.

Dastlab, tizim ma’murlari suqilib kirishlarni konsol oldida o‘tirib va foydalanuvchi harakatlarini tahlil qilish orqali aniqlashgan. Ular, hujumni quyidagilarga e’tibor berish orqali aniqlay olishgan, ta’tilda bo‘lishi kerak bo‘lgan foydalanuvchi lokal tarmoq orqali tizimga kirganda, kamdan-kam hollarda ishlatiladigan printer aktiv holda ishlatilganda. Qachonlardir suqilib kirishlarni aniqlovchi ushbu usul samarali bo‘lgan, shuning bilan birgalikda bu usul muayyan vaziyatlarga qaratilgan va mashstablik hususiyatiga ega bo‘lmagan.

Axborot va tarmoq texnologiyalari juda tez rivojlanmoqda va o‘zgarib bormoqda bunday hollarda statik himoyalash vositalari, kirish huquqlarini cheklash hamda autentifikatsiya tizimlari ko‘p hollarda samarali himoyani ta’minlay olmaydi. Qisqa muddat ichida xavfsizlik buzilishini aniqlovchi va oldini oluvchi dinamik usullar talab qilinadi. Ana shunday tizimlardan biri bo‘lib, an’anaviy foydalanish huquqlarini nazorat qiluvchi modellar aniqlay olmaydigan buzilishlarni kuzatishga imkon beruvchi hujumlarni aniqlash texnologiyasi hisoblanadi.

Xujumlarni aniqlashni hisoblash yoki tarmoq resurslariga yo‘naltirilgan shubxali harakatlarni identifikatsiyalash va ularga reaktsiya ko‘rsatish jarayoni.

Texnologiyalarning samaradorligi ko‘p jihatdan qabul qilingan axborotni tahlil qilishda foydalanilgan usullarga bog‘liq. Ayni paytda, statistik usul bilan bir qatorda ekspert tizimlari va neyron tarmoqlar kabi yangi usullardan foydalanilmoqda.

Hozirda xujumlarni aniqlash tizimlarida 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’yekt xarakteriga moslash. Ushbu usuldan foydalanishdan avval tahlil qilinayotgan tizimning har bir sub’yekti uchun profillar aniqlab olinadi. Foydalanilgan profil mezoniga mos kelmagan hatti xarakatlar ruxsat etilmagan xatti harakat deb qabul qilinadi. Statistik usullar universal xisoblanadi ular tizimga bo‘ladigan xujumlar va zaifliklar xaqida bilimlarni talab etmaydi. Biroq ulardan foydalanganda ba’zi bir qiyinchiliklar paydo bo‘lishi mumkin, misol uchun ruxsat etilmagan xarakatlarni normal xarakat deb ko‘rsatib qo‘yish mumkin. Shuning uchun, statistik tahlil qilish bilan birgalikda qo‘shimcha usullar ishlatiladi.

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 muhim afzalligi - yolg‘on trevoganing umuman bo‘lmasligi. Ekspert tizimlarini doimo faol saqlash uchun foydalaniladigan ma’lumotlar bazalarini yangilab borish zarur. Ushbu usulning kamchiligi noma’lum bo‘lgan xujumlarni bartaraf etish imkoniyatining mavjud emasligi. Agar ma’lumotlar bazasidan xujumni bir oz o‘zgartirib qo‘yilsa bu uni aniqlashda muhim to‘siq bo‘lib qoladi. Shuni ta’kidlash zarurki oddiy IDS faqatgina ma’lum bo‘lgan xujumlarni o‘z vaqtida aniqlaydi. Ular xam antivirus dasturlarining rejimida ishlaydi: ma’lumlari-aniqlanadi, noma’lumlari-aniqlanmaydi. Joriy hodisalarni tahlil qilishda sodir bo‘lgan xujumlar ham xisobga olinishi mumkin, bu xujumlarni identifikatsiya qilishga va kelajakda sodir bo‘ladigan xodisalarni prognoz qilishga imkon yaratadi.

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

Neyron tarmoqlaridan foydalanish ekspert tizimlarining yuqorida keltirilgan muammolarni bartaraf etishning bir usuli hisoblanadi. Ekspert tizimlari foydalanuvchiga ko‘rilayotgan xarakteristikalar ma’lumotlar bazasidagi qoidalarga mos kelishi yoki mos kelmasligi xususida aniq javob bera olsa, neyrotarmoq axborotni tahlillaydi va ma’lumotlarni aniqlashga o‘rgangan xarakteristikalariga mos kelishini baxolash imkoniyatini taqdim etadi.

Zamonaviy hujumlarni aniqlash tizimlarining tuzilishi

Hujumlarni aniqlash tizimlari (IDS) - himoyalangan kompyuter tizim (hisoblash tarmoq)larining turli nuqtalaridan ma’lumot yig‘uvchi, ushbu ma’lumotlarni buzishga urinishlarni aniqlash uchun tahlil qiluvchi va haqiqiy himoyaning buzilish(suqilib kirish)larini aniqlovchi tizim.

Zamonaviy aniqlash tizimlari mantiqan quyidagi asosiy elementlarga ajratiladi: axborot yig‘uvchi quyi tizimi, tahlil qiluvchi quyi tizimi va hisobot taqdim qiluvchi modul.

Axborot yig‘uvchi quyi tizim himoyalanayotgan tizim ishi haqida boshlang‘ich ma’lumotlarni to‘plash uchun ishlatiladi.

Tahlil qiluvchi quyi tizim (aniqlash) himoyalangan tizimga nisbatan hujum va suqilib kirishlarni qidirishni amalga oshiradi.

Hisobotlarni taqdim qiluvchi quyi tizim (foydalanuvchi interfeysi) DNS foydalanuvchilariga himoyalanayotgan tizim holatini kuzatib borish imkonini beradi.

Axborot to‘plash quyi tizimida himoyalanayotgan tizim ishi haqida ma’lumotlar to‘planadi. Axborot to‘plash uchun avtonom modullar-datchiklardan foydalaniladi. Ishlatiladigan datchiklar soni har xil bo‘ladi va himoyalanayotgan tizimning hususiyatlariga bog‘liq bo‘ladi. IDSdagi datchiklari to‘planadigan ma’lumotlar turiga qarab sinflanadi. Axborot tizimlarining umumiy tuzilishiga muvofiq quyidagi turlarga ajratiladi:

- ilova sensorlari - himoyalanayotgan tizimning dasturiy ta’minoti ishi haqida ma’lumot to‘playdi;

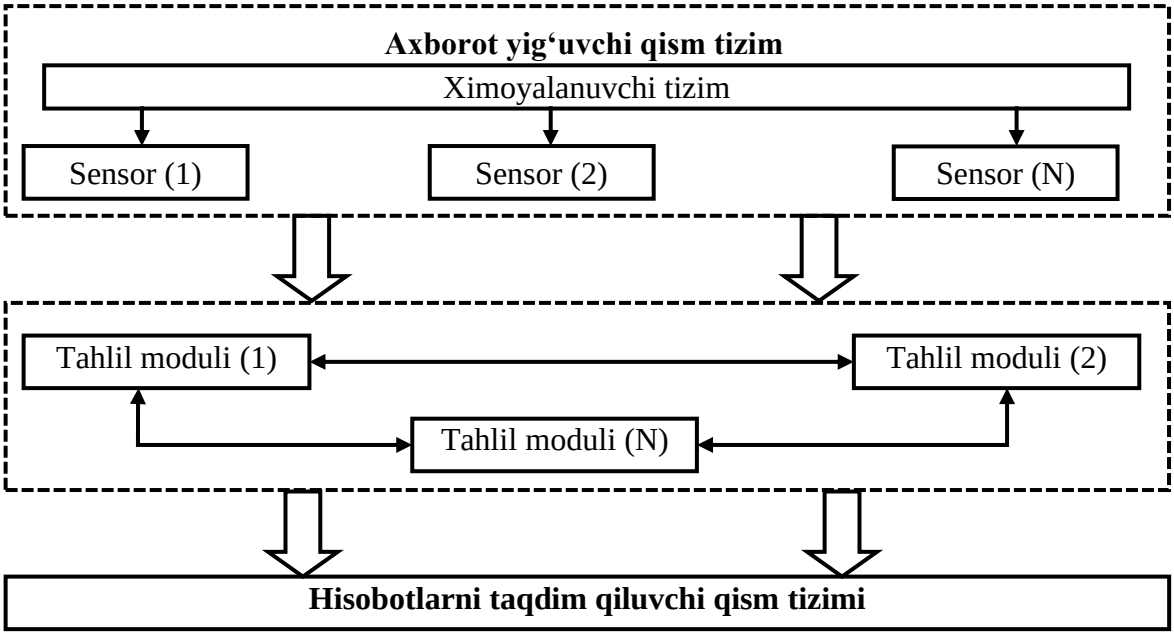
- host sensorlari - himoyalanayotgan tizim ishchi stansiyasi faoliyati haqida ma’lumot to‘playdi;

- tarmoq sensorlari - tarmoq trafigini baholash uchun ma’lumotlar to‘playdi;

- tarmoqlararo sensorlar - tarmoqlar orasidagi almashinuvchi ma’lumotlar xususiyatlarini o‘z ichiga oladi.

Tahlil qiluvchi qism tizimi - bir yoki bir necha tahlil modullari, analizatorlarni o‘z ichiga oladi. Bir necha analizatorlarning mavjudligi aniqlash samaradorligini oshirish uchun kerak. Har bir analizator muayyan turdagi hujumlar yoki suqilib kirishlarni izlashni amalga oshiradi. Analizator uchun kirish ma’lumotlari bo‘lib, axborot yig‘uvchi quyi tizimdan yoki boshqa analizatordan olingan axborot xizmat qiladi. Zamonaviy IDS larning tahlil qiluvchi quyi tizimlarida foydalanilgan usullarni ikki yo’nalishga ajratish mumkin: birinchisi

ximoya qilinayotgan tizimda anomal xodisalarni aniqlashga, ikkinchisi ruxsat etilmagan xatti harakatlarni qidirishga yo‘naltirilgan [5].



1.2-rasm. Hujumlarni aniqlash tizimi arxitekturasi

Ma’lumotlarni taqdim qiluvchi quyi tizim, ximoya qilinayotgan tizim holati haqida xabardor qilish uchun zarur. Ba’zi bir tizimlarda, ximoya qilinayotgan tizimning muayyan quyi tizimini nazorat qiluvchi foydalanuvchilar guruhi mavjud. Shuning uchun, bunday IDSlarda foydalanishlarni cheklash, vakolatlarni cheklashlardan foydalaniladi.

Javob berish usuliga ko‘ra:

- aktiv tizimlar (suqilib kirishlarni oldini olish tizimlari) - tahdid aniqlanganda faol choralarlarni amalga oshiradi (tahdid manbasini bloklash, tahdid manbasini skanerlash, himoyalangan infratuzilmaning barcha ulanishlarini yopish va boshqalar);
- passiv tizimlar (suqilib kirishlarni aniqlash tizimlari) – ma’lumotlarni yig‘ish va tahlil qilish, paydo bo‘lgan tahdid to‘g‘risida mas’ul shaxslarni yoki boshqa tizimlarni xabardor qilish.

Arxitektura bo‘yicha:

- taqsimlangan - tizim datchiklardan, markaziy tugun, boshqaruv va o‘zaro aloqa interfeysidan iborat;

- markazlashtirilgan, bunda barcha hisob-kitoblar bitta tugun doirasida amalga oshiriladi.

Monitoring obyektining turi bo‘yicha:

- tarmoq IDS, bunda monitoring obyekti tarmoq segmenti hisoblanadi;
- tugun IDS, bunda monitoring obyekti tarmoqdagi tugun hisoblanadi;
- gibrid - tugun va tarmoq hususiytalariga ega IDS.

Tahlil texnologiyasi bo‘yicha:

- holatni saqlagan holda, oldingi voqealar haqida ma’lumot saqlanadi va qaror qabul qilishda hisobga olinadi;
- holatni saqlamagan holda, har bir hodisa boshqalardan mustaqil ko‘riladi.

Tahdidni aniqlash usuliga ko‘ra:

- signaturali tizimlar;
- mashinali o’qitish tizimlari;
- anomaliyalarni aniqlash tizimlari;
- protokoldagi buzilishlarni aniqlash tizimlari.

Suqilib kirishlarni aniqlash usullari va yo’nalishlarini xususiyati:

- Zamonaviy IDSlarning tahlil qiluvchi quyi tizimlarida foydalanilgan usullarni ikki yo‘nalishga ajratish mumkin: birinchisi ximoya qilinayotgan tizimda anomal xodisalarni aniqlashga, keyingisi ruxsat etilmagan hatti xarakatlarni qidirishga yo‘naltirilgan. Har bir yo‘nalish o‘z afzalliklari va kamchiliklariga ega, shuning uchun ko‘plab mavjud IDSlarda ushbu usullarni sinteziga asoslangan holda kombinatsiyalangan yechimlardan foydalaniladi. Anomaliyalarni aniqlashda foydalanilgan usullar, tizim ishida o‘zgarishlarga olib keluvchi jarayonlar tajovuzkor tomonidan amalga oshirilmayotganligini aniqlashga yo‘naltirilgan. Anomaliyalar qidiruv usullari quyidagi jadvallarda ko‘rsatilgan.

Usullar ikki guruhga ajratiladi: nazorat ostidagi ta’lim bilan amalga oshiriladigan (“o‘qituvchi yordamida o‘qitish”) va nazoratsiz ta’lim orqali amalga oshiriladigan (“o‘qituvchi yordamisiz o‘qitish”). Ular orasidagi asosiy farq nazorat

ostidagi ta’lim usullarida baxolashni belgilangan hususiyatlaridan foydalaniladi. O’qitish vaqti belgilanadi.

Nazoratsiz ta’limda baxolash hususiyatlari vaqt davomida o‘zgarishi mumkin, o‘qitish jarayoni doimiy amalga oshiriladi.

1.2-jadval

Anomaliyalarni aniqlash - nazorat ostidagi ta’lim (“o‘qituvchi yordamida o‘qitish”)

Aniqlash usullari	**Foyadalaniladigan tizimlar**	**Usullar tavsifi**
Qoidalarni modellashtirish	W & S	Aniqlash tizimi, o‘quv jarayoni davomida tizimning normal holatini ifodalovchi qoidalar majmuini shakllantiradi. Ruxsatsiz harakatlarni qidiruv bosqichida, tizim olingan qoidalardan foydalanadi va yetarlicha muvofiqlik aniqlanmasa anomal holat aniqlanganligi haqida signal beradi.
Tasvirlovchi statistika	IDES, NIDES, EMERLAND, JiNao, HayStack	O‘qitish himoya qilinayotgan tizimning ko‘plab ko‘rsatkichlarini oddiy tasvirlovchi statistikadan maxsus strukturaga jamlashga asoslanadi. Anomaliyalarni aniqlash uchun ikki vektor ko‘rsatkichlar -joriy va saqlangan qiymatlar o‘rtasidagi “masofa” hisoblanadi. Olingan masofa yetarlicha katta bo‘lsa tizimdagi holat anomaliya hisoblanadi.
Neyron tarmoqlar	Hyperview	Ishlatiladigan neyron tarmoqlarning tuzilishi turlicha. Lekin barcha ta’lim berish hollari, tizimning normal holatini

		ifodalovchi ma’lumotlari asosida amalga oshiriladi. Olingan neyron tarmoq keyinchalik tizimning anomalligini baholash uchun ishlatiladi. Neyron tarmog‘ining chiqishdagi ma’lumotlari anomaliya borligini bildiradi.

1.3-jadval

Anomaliyalarni aniqlash - nazoratsiz ta’lim orqali (“o‘qituvchi yordamisiz o‘qitish”)

Aniqlash usullari	**Foyadalaniladigan tizimlar**	**Usullar tavsifi**
Ko‘plab holatlarni modellashtirish	DPEM, JANUS, Bro	Tiziming normal ko‘rinishi, chegaralangan holatlar va ular orasidagi o‘tish majmui ko‘rinishida tasvirlanadi.
Tasvirlovchi statistika	MIDAS, NADIR, Haystack, NSM	Nazorat ostidagi ta’lim usuliga o‘xshash.

1.4-jadval

Ruxsat etilmagan hatti xarakatlarni aniqlash - nazorat ostidagi ta’lim (“o‘qituvchi yordamida o‘qitish”)

Aniqlash usullari	**Foyadalaniladigan tizimlar**	**Usullar tavsifi**
Hollatlarni modellashtirish	USTAT, IDIOT	Suqilib kirish holat ketma-ketligi ko‘rinishida tasvirlanadi, holat - himoya qilinayotgan tizimning baholash hususiyatlarining qiymatlar vektori. Ushbu ketma-ketlikning borligi suqilib

		kirish mavjudligi uchun zarur va yetarli shart. Suqilib kirishni tasvirlashning asosan ikki usuli mavjud: 1) hodisalarni oddiy zanjir ko‘rinishida; 2) Petr tarmoqlaridan foydalanib, tugunlar – hodisalar ko‘rinishida.
Ekspert tizimlar	NIDES, EMERLAND, MIDAS, DIDS	Ekspert tizimlar suqilib kirish jarayonini turli qoidalar majmui ko‘rinishida tasvirlaydi. Tez-tez ishlab chiqarish tizimlari ishlatiladi.
Qoidalarni modellashtirish	NADIR, HayStack, JiNao, ASAX, Bro	Ekspert tizimilarining oddiy varianti.
Sintaktik tahlil	NSM	Aniqlash tizimi tomonidan, quyi tizimlar va himoya qilinayotgan kompleks tizimlari o‘rtasida uzatiladigan simvollar kombinatsiyasini aniqlash maqsadida ularni sintaktik qismalrga ajratiladi.

Ikkinchi yo‘nalishning maqsadi (suqilib kirishlarni aniqlash) – suqilib kirishni amalga oshirish bosqichi sifatida aniqlangan (xavfsizlik administrator yoki IDSni o‘qitish vaqtidagi ekspert)lardan, hodisalar ketma ketligini qidirsih. Suqilib kirishlarni qidiruv usullari jadvalda ko‘rsatilgan. Hozirgi kunda, faqat nazorat ostidagi ta’lim usuli farqlanadi.

Hozirgi paytda amalga oshirilgan IDSlardagi usullar obrazlarni aniqlashning umumiy g‘oyalariga asoslanadi. Ularga ko‘ra, ekspert bahosi asosida anomaliyani aniqlash uchun normal faoliyat olib borayotgan axborot tizimining obrazi shakllantiriladi. Uning o‘zgarishi tizimning anomal faoliyat olib borayotganini bildiradi. Anomaliya aniqlangandan va uning darajasi baxolangandan so‘ng o‘zgarishning tabiati haqida ma’lumotlar shakllantiriladi: ular suqilib kirishning

oqibatlarimi yoki ruxsat etilgan harakatlarmi. Suqilib kirishlarni aniqlash uchun obraz(signatura)lardan foydalaniladi, lekin bunda xujumchining oldindan ma’lum bo‘lgan harakatlarigina bartaraf etiladi.

Birinchi navbatda, IDS larda ruxsat etilmagan faollikni aniqlash uchun turli usullar ishlatiladi. Tarmoqlararo ekran (brandmauyer) orqali amalga oshiriladigan hujumlar bilan bog‘liq muammolar mavjud. Tarmoqlararo ekran muayyan xizmatlar (portlar)ga murojaat qilishga ruxsat beradi yoki rad etadi, biroq ochiq port orqali o‘tadigan axborot oqimini nazorat qilmaydi. Buzg‘unchi o‘zini sezilmagan deb o‘ylagan bir vaqtda, IDS o‘z navbatida tizimga yoki tarmoqqa bo‘lgan xujumni aniqlashga va xavfsizlik administratoriga bu haqda xabar berish uchun harakat qiladi.

Buni uyni o‘g‘rilardan himoya qilish bilan qiyoslash mumkin. Eshik va derazalarni qulflash – tarmoqlararo ekran. Buzulish haqida ogohlantiruvchi signalizatsiya bu IDS ga mos keladi.

IDS tasniflash uchun turli yo‘llar mavjud. Shunday qilib, javob berish usuli bo‘yicha passiv va aktiv IDS larga ajratiladi. Passiv IDS lar shunchaki hujumni ro‘yhatga oladi, ma’lumotlarni qayd jurnaliga yozib qo‘yadi va ogohlantirish beradi. Aktiv IDS lar hujumga qarshi harakatlarni amalga oshirishga harkat qiladi, masalan, tarmoqlararo ekranlar konfiguratsiyasini o‘zgartirish va marshrutizatorlar ro‘yhatini generatsiya qilish orqali. Yuqoridagi o‘xshashlikni davom ettiradigan bo‘lsak, uyda signal tizimi o‘g‘rilarni to‘xtatish uchun sirena ovozini faollashtirsa- bu aktiv IDS, agar militsiyaga signal yuborsa - bu passiv IDS ga mos keladi.

Hujumlarni aniqlash usuli bo‘yicha signature based va anomaly based tizimlari farqlanadi. Birinchi tur oldindan o‘rnatilgan hujumlar signaturasi bazasi bilan ma’lumotlarni taqqoslashga asoslangan. O’z navbatida, hujumlarni turiga ko‘ra tasniflash mumkin (masalan, Ping-of-Death, Smurf). Lekin, bu turdagi tizimlar hujumlarni yangi, noma’lum turlarini aniqlay olmaydi. Ikkinchi tur hodisalar davriyligini nazorat qilishga yoki statistik anomaliyalarni aniqlashga asoslangan. Ushbu tizim hujumlarning yangi turlarini aniqlashga qaratilgan. Lekin, uning kamchiligi – doimiy o‘qitish olib borilishi zarur. Uylarni himoya qilish

misolida IDS tizimlari o‘rnida qo‘shnilar olinadi, no‘malum shaxslarga diqqat bilan qaraydilar, ular uyga kim kelganligi va ko‘chada favqulodda vaziyat haqida ma’lumot to‘playdilar. Bu anomalous IDS turiga mos keladi.

Ikkinchi tur tizimlar, host-based, ma’lum bir hostda buzg‘unchining harakatlariga qarshi reaksiya ko‘rsatish, tahlil qilish va aniqlash uchun mo‘ljallangan. Tizim himoyalangan xostda joylashgan bo‘lib, unga qarshi amalga oshirilayotgan harakatlarni tekshiradi va aniqlaydi. Uchinchi tur IDS, application-based, ma’lum bir dasturlardagi muammolarni qidiruviga asoslangan. Shuningdek gibrid IDS lar mavjud, ular turli tizimlar birlashmasidan tashkil topadi.

Zamonaviy IDSlarning ishlashi va turli hujum turlari

So‘nggi paytlarda distributed IDS (dIDS) deb nomlanuvchi tizimlar haqida ko‘plab nashrlar chiqmoqda. dIDS ko‘plab IDS lardan tashkil topgan, ular katta tarmoqning turli qismlarida joylashgan, markaziy boshqaruv serveri va bir-biri bilan bog‘langan. Bunday tizimlar turli IDS lardan hujum haqida ma’lumotlarni markazlashgan holda ishlanish hisobiga korporativ tarmoqlar xavfsizligini kuchaytiradi. dIDS quyidagi kichik tizimlardan iborat: markaziy tahlil serveri, tarmoq agentlari, hujum haqida ma’lumot yig‘uvchi server.

Markaziy tahlil serveri odatda Web-serverlar va ma’lumotlar bazalaridan tashkil topgan bo‘lib, hujum haqida ma’lumotlarni saqlashga va ma’lumotlarni qulay Web-interfeys orqali qayta ishlashga imkon beradi.

Tarmoq agentlari - dIDSning eng muhim qismlaridan biri. Katta bo‘lmagan dastur bo‘lib, uning maqsadi hujum haqida markaziy tahlil serveriga xabar qilish.

Hujum haqida ma’lumot yig‘ish serveri - dIDStizimining markaziy tahlil serverida mantiqiy tashkil etilgan qismi. Server tarmoq agentlarida olingan ma’lumotlarni guruhlash uchun parametrlarni belgilaydi. Guruhlash quyidagi parametrlar orqali amalga oshirilishi mumkin [5]:

- buzg‘unchining IP- manzili;
- qabul qiluvchining porti;
- agent raqami;
- sana, vaqt;

- protokol;
- hujum turi, va hokazo.

1-bob bo‘yicha xulosa

Magistrlik dissertatsiya ishining birinchi bobida axborot tizimlarida tarmoq xavfsizligidagi tahdidlar va ulardan himoyalanish usullari haqida umumiy ma’lumotlar berilib, quyidagi natijalar olindi:

- axborot tizimida saqlanadigan va ma’lumotlarni uzatish jarayonida axborotni xavfsizligiga nisbatan tarmoqdan bo‘ladigan tahdidlar tavsifi va tasnifi ko‘rib chiqildi;

- tajavuzkor tomonidan tashkilotning tarmog‘iga tashqaridan bo‘ladigan hujumlarni amalga oshirish bosqichlari hamda tasnifi ko‘rib chiqildi;

- axborot tizimlarida mavjud zaifliklar va kamchiliklardan foydalanib, himoyalash tizimining foydalanuvchanligini buzilishga qaratilgan suqilib kirishlarni aniqlash va bartaraf etish tizimlarida qo‘llaniladigan yondashuvlar tadqiq va tahlil qilindi.

2 BOB. SUN’IY IMMUN TIZIMIGA ASOSLANGAN ANOMAL SO‘ROVLARNI ANIQLASH TIZIMLARI

2.1 Anomal so‘rovlarni aniqlashda qo‘llaniladigan ma’lumotlar to‘plamining tahlili

Mashinali o‘qitish tizimlarining samaradorligini o‘qitish va keyingi sinovdan o‘tkazish uchun tegishli ma’lumotlar to‘plamlari (Datasets) qo‘llaniladi. Odatda, bu ma’lumotlar to‘plamlari quyidagi tuzilishga ega:

Ushbu bo‘limda ma’lumotlar to‘plamlari (Datasets) hujumlarni aniqlash tizimlarida adaptiv algoritmlarni o‘qitish va ishlashini baholashning eng muhim usullaridan biri sifatida ko’rib chiqilgan.

Tadqiq va tahlil etishda tarmoq protokollari bilan ishlash imkoniyatiga ega bo‘lganlar quyidagi ma’lumotlar to‘plamlari tanlab olingan:

- NSL-KDD ISCX Dataset (ishlash protokollari TCP, UDP, ICMP);
- CSIC 2010 Dataset (ishlash protokollari HTTP/1.1);
- Enron Dataset (ishlash protokollari SMT).

Har bir ma’lumotlar to‘plami “kalit (xususiyat)-qiymat” turidagi ma’lum bir protokolga xos bo‘lgan cheklangan xususiyatlarni o‘z ichiga oladi.

Tasniflash muammosi nuqtai nazaridan har bir so‘rovni ikkita sinfdan biriga kiritish mumkin:

- normal holat - tizim uchun potentsial xavfli bo‘lmagan so‘rovlar sinfi;
- anomal holat - bajarilishi natijasida tizimning noto‘g‘ri ishlashiga olib kelishi mumkin bo‘lgan so‘rovlar sinfi.

Formal ravishda, anomal so‘rovlarni aniqlashning asosiy vazifasi tasniflash muammosini hal qilishni talab etadi, ya’ni funksiya gipotezasini ishlab chiqish:

$$h_\theta^{(i)}(x) = Pr[y = i|x, \theta], x \in P,$$

bu yerda hP, so‘rovlar $P = \{p_j\}$ xususiyatlar to‘plamining $C = \{'normal', 'abnormal'\}$ to‘plamlar sinfiga akslantirilishi, Θ esa mashinali o‘qitish ob’yektining parametr vektori hisoblanadi. Bunda, $\in$ so‘rov

xususiyatlarining n o‘lchovli fazosidagi vektori, $x \in P, Pr$ - xususiyat vektori, $y \in$ esa sinfning sonli kodi hisoblanadi.

Bunda so‘rovlarni tasniflash muammosini hal qilish uchun quyidagi vazifalarni hal qilish talab etiladi:

1. $h(x)$ funksiya tomonidan amalga oshiriladigan algoritmni tanlash. Bu yerda $h(x)$ funksiyasining roli muvofiqlikni tahlil qilish mexanizmidan foydalangan holda sun’iy intellekt texnologiyasini amalga oshirishdan iborat, θ parametrlar to‘plami esa mashinali o‘qitish algoritmi yordamida iterativ tarzda aniqlanadi.

2. Yakuniy tizimga bo‘lgan so‘rovlarni tavsiflovchi P xususiyatlar to‘plamini tanlash.

Sun’iy immun tizimi uchun adaptiv algoritmni ishlab chiqishdan oldin, undan tasniflash masalasini hal qilish uchun zarur xususiyatlarni ajratib olish imkonini beruvchi formal so‘rov modelini ishlab chiqish kerak. Yuqorida ko‘rsatilgan to‘plamlarni tanlashda tasniflash uchun zarur bo‘lgan xususiyatlar mavjud [6].

Yuqorida aytib o‘tilganidek, barcha ma’lumotlar to‘plami kamida ikkita kichik to‘plamdan iborat:

- o‘qitish tanlanmasi (training dataset) - adaptiv algoritmni shakllantirish jarayonida maksimal natijaga erishish maqsadida parametrlarni tanlash amalga oshiriladi;
- testlash tanlanmasi (testing dataset) - bunda adaptiv algoritmni o‘rganish sifati tekshiriladi.

Ushbu to‘plamlarning har birida obyektlarning ko‘rsatkichlari bir xil. Tanlangan ma’lumotlar to‘plamida formal so‘rov modellarini (ko‘rsatkichlarni) ko'rib chiqing.

NSL-KDD Dataset ma’lumotlar to‘plami

NSL-KDD ma’lumotlar to‘plamining avlodi KDD99 Dataset xisoblanadi.. KDD99 suqulib kirishni aniqlash tizimlari uchun amalda birinchi ma’lumotlar to‘plami standarti xisoblanib, qiyosiy ma’lumotlarni taqdim etish uchun yaratilgan.

suqulib kirishni aniqlash tizimlarida adaptiv algoritmlarni sinovdan o'tkazish.

Suqulib kirishlarni aniqlash tizimlarining rivojlanishi tufayli KDD99 ni amalga oshirishda ko'plab kamchiliklar aniqlandi, ular keyinchalik NSL-KDD ma’lumotlar to‘plamini joriy etish orqali bartaraf etildi. NSL-KDD DataSet KDD99 ga nisbatan bir qator afzalliklarga ega, ular orasida quyidagilar mavjud:

- chastota xarakteristikalarining (ortiqchalik, takrorlanish) moslashuvchan mexanizmga ta’sirini bartaraf etish maqsadida bir qator yozuvlarni o'chirish;
- test va o'quv to‘plamlarini shakllantirishga kuchliroq yondashuv va boshqalar.

NSL-KDD ma’lumotlar to‘plamining tarkibi va tavsifi 2.1 va 2.2 jadvalda keltirilgan.

2.1 Jadval

NSL-KDD Dataset ma’lumotlar to‘plami

№	To‘plamning nomi	Tavsifi
1	*KDDTrain+*	hujum yorliqlari va murakkablik darajasi bilan o‘quv tanlovi
2	*KDDTrain+20%*	KDDTrain+ ning 20% kichik to‘plami
3	*KDDTest+*	hujum belgilari va murakkablik darajasi bilan to‘plam tekshiruvi
4	*KDDTest-21*	to‘plam KDDTest+ 21 qiymatidan yuqori bo‘lgan hujumlar daraja qaydini o‘z ichiga olmaydi

2.2 - jadval

NSL-KDD Dataset yozuvlarni to‘plamlar bo‘yicha taqsimlanishi

To‘plamning nomi	*Soni*					
	Yozuvlarning miqdori	*Normal so‘rovlar*	*DoS*	*Probe*	*U2R*	*R2L*
KDDTrain+20%	25192	13449	9234	2289	11	209
		53.39%	36.65%	9.09%	0.04%	0.83%
KDDTrain+	125973	67343	45927	11656	52	995
		53.46%	36.46%	9.25%	0.04%	0.79%

KDDTest+	22544	9711	7458	2421	200	2754
		43.08%	33.08%	10.74%	0.89%	12.22 %

NSL-KDD Dataset ob’yektlar ulanishlar - ma’lum bir vaqt oralig‘ida o‘rnatilgan (TCP, UDP, ICMP) paketlar ketma-ketligi bo'lib, u ma’lumotlar oqimini manba IP-manzildan belgilangan IP-manzilga ma’lum bir maxsus protokolga muvofiq ifodalaydi.

Ma’lumotlar to‘plami 4 toifa tahdidni o'z ichiga oladi:

- Denial of Service (dos). Buzg‘unchi ma’lum bir protokol (Back, Land, Neptun, Pod, Smurf, Teardrop, Apache2, Udpstorm, Processtable, Worm) orqali tasdiqlangan foydalanuvchilar uchun ma’lum bir xizmatga kirishni cheklaydigan hujumlar to‘plami.
- *Remote to Local (r2l).* Buzg‘unchi foydalanuvchining lokal mashinasiga tashqaridan kirishga harakat qiladigan hujumlar to‘plami (Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named)
- *User to Root (u2r).* Jabrlanuvchining mashinasiga kirish huquqiga ega bo‘lgan buzg‘unchi ko‘proq imtiyozli foydalanuvchi huquqlarini olishga harakat qiladigan hujumlar to‘plami (Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps).
- *Probe.* Buzg‘unchi foydalanuvchi infratuzilmasi (Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint) haqida ma’lumot olishga harakat qiladigan hujumlar to‘plami.

NSL-KDD Dataset vektorning o‘lchami (so‘rov uchun xususiyat soni) 43 bo'lsa-da, haqiqiy ish uchun 41 xususiyat ishlatiladi. 42-xususiyat tahdid toifasini, 43-atribut esa hujumning murakkabligini (eng oddiydan eng murakkabgacha) ifodalaydi. Shunday qilib, NSL-KDD Dataset ma’lumotlar to‘plami uchun formal so‘rov modelini 41 o‘lchovli vektor ifodalaydi [7].

NSL-KDD Dataset so‘rovlarini yozish xususiyatlarining to‘liq ro‘yxati 2.3-jadvalda keltirilgan.

2.3 - jadval

NSL-KDD Dataset so‘rovlar yozuvlarining xususiyatlari.

Xususiyat	Tavsifi	Xususiyat	Tavsifi
1. duration	Ulanish davomiyligi	*22. is guest login*	agar "guest" bo‘lsa, aks holda 0
2. protocol type	Protokol turi (tcp, udp va h.k.)	*23. count*	oxirgi ikki soniya ichida joriy ulanish bilan bir xil xostga ulanishlar soni
3. service	Belgilangan manzil xizmati (telnet, ftp va h.k.)	*24. srv count*	oxirgi ikki soniya ichida joriy ulanish bilan bir xil xizmatga ulanishlar soni
4. flag	Ulanishning holat bayrog‘i	*25. serror rate*	“SYN" paketidagi xatolik bilan ulanishlarning %
5. source bytes	Belgilangan manzilga yuborilgan baytlar soni	*26. srv serror rate*	“SYN" paketidagi xatolik bilan ulanishlarning %
6. destination Bytes	Yuboruvchidan jo‘natilgan baytlar soni	*27. rerror rate*	“REJ" paketidagi xatolik bilan ulanishlarning %
7. land	Agar ulanish –dan/-ga bir xil bo‘lsa xost/port, aks holda 0	*28. srv rerror rate*	“REJ" paketidagi xatolik bilan ulanishlarning %
8. wrong fragment	Xato bo‘lgan fragmentlar soni	*29. same srv rate*	Xuddi shu xizmatga ulanishlar %
9. urgent	Shoshilinch paketlar soni	*30. diff srv rate*	Turli xizmatlarga ulanishlar %
10. hot	“Muxim” indikatorlar soni	*31. srv diff host rate*	Turli xostlarga ulanishlar %
11. failed logins	Muvaffaqiyatsiz urunishlar soni	*32. dst host count*	Bir xil portlarga ega ulanishlar soni
12. logged in	agar chiqish muvaffaqiyatli	*33. dst host srvcount*	Bir xil portlarga va xizmatlarga ega

	bo‘lsa 1,aks holda 0		ulanishlar soni
13. compromised	Sohtalashtirilgan shartlar soni	*34. dst host same srv rate*	Bir xil xostlarga va xizmatlarga ega ulanishlar %
14. root shell	agar “root” xuquqi berilgan bo‘lsa 1, aks holda 0	*35. dst host diff srv rate*	Joriy xostdagi turli xizmatlarning %
15. su attempted	“su root” muvaffaqiyatli bo‘lsa 1, aks holda 0	*36. dst host same src port rate*	Joriy xostdagi bir xil portga ega ulanishlarning %
16. root	“root” sessiyalar soni	*37. dst host srv diff host rate*	Boshqa xostlardan olingan joriy xizmat ulanishlarining %
17. file creations	Fayllar yaratish operatsiyalari soni	*38. dst host serror rate*	S0 xatosi bo‘lgan joriy xostga ulanishlarning %
18. shells	Ishga tushirilgan qobiqlar soni	*39. dst host srvb serror rate*	S0 xatosi bo‘lgan joriy xostga va xizmatga ulanishlarning %
19. access files	Fayllarga kirish operatsiyalari soni	*40. dst host rerror rate*	RST xatosi bo‘lgan joriy xostga ulanishlarning %
20. outboun dcmds	Ftp sessiyasida chiquvchi buyruqlar soni	*41. dst host srv rerror rate*	Har qanday RST xatosi bo‘lgan joriy xostga va xizmatga ulanishlarning %
21. is hot login	agar avtorizatsiya “issiq” bo‘lsa 1, aks holda 0		

CSIC 2010 HTTP ma’lumotlar to‘plami

CSIC 2010 minglab avtomatik tarzda yaratilgan Web-so‘rovlarni o‘z ichiga olgan HTTP/1.1 protokoli (RFC 2616) uchun maxsus dasturiy ta’minot yordamida olingan ma’lumotlar to‘plamidir.Ushbu to‘plam suqulib kirishlarni

aniqlash tizimlarida ishlashning bir qismi sifatida moslashuvchan algoritmlarga so‘rovlar orqali Web-hujumlarni sinab ko‘rish uchun ishlatiladi.Algoritm Web-xavfsizlik kontekstida moslashuvchan tizimlarni o‘qitish nuqtai nazaridan ahamiyatsizligi, shuningdek, CSIC ko‘proq yo‘naltirilganligi sababli bir qator to‘plamlarni (huddi shu KDD99) almashtirish uchun mo‘ljallangan shunchaki multiprotokolda emas,balki ma’lum bir HTTP / 1.1 protokolida.Ushbu to‘plam Internet tarmog‘idagi elektron platformalar faoliyatining bir qismi sifatida keladigan bir nechta so‘rovlarni taqlid qiladi *CSIC 2010 HTTP* ma’lumotlar to‘plami tarkibi 2.4 jadvalda keltirilgan

2.4 - jadval

CSIC 2010 HTTP ma’lumotlar to‘plami

№	To‘plamning nomi	Yozuvlar soni	Tavsifi
1	*Anomalous test*	119586	Anomal so‘rovlar to‘plami
2	*Normal training*	104001	Test so‘rovlar to‘plami
3	*"Full" dataset*	223585	Anomal va test so‘rovlarining to‘liq to‘plami (odatiy trafik)

Barcha http so‘rovlari anomal va anomal emas deb belgilangan.

Anomal so‘rovlar quyidagilarni o‘z ichiga oladi:

- *SQL* in’yektsiyalar;
- buferni to‘ldirish buyruqlari (*buffer overflow*);
- ma’lumot yig‘ish buyruqlari(*probe operations*);
- Web-ilova ishlayotgan fayl tizimining yo‘llarini namoyon qilish uchun buyruqlar;
- *CRLF* in’yektsiyalar;
- *XSS* hujumlar;
- fayllarni masofadagi serverga yuklash buyruqlari;
- uzatiluvchi parametrlarni soxtalashtirish.

CSIC 2010 HTTP/1.1 HTTP/1.1 protokoli ostida ishlaydigan tarmoq

hujumlarini aniqlash tizimlarini sinovdan o‘tkazish standartlaridan biri hisoblanadi.

So‘rovni generatsiya qilishda tavsiflangan bir necha bosqichlarni o‘z ichiga oladi va umumiy holda uchta turdagi anomal so‘rovlarni o‘z ichiga oladi:

1. Statik hujumlar, bunda yashirin yoki mavjud bo‘lmagan parametrlarni qabul qilish taqlid qilinadi. Bu so‘rovlar fayllarga mutlaq yo‘llarni, URL parametrlaridagi sessiya identifikatorlari,tarkibiy tuzilma va odatiy fayllarni qabul qilish, va boshqalarni o‘z ichiga oladi.

2. Dinamik hujumlar, bunda so‘rov argumentlarida modifikatsiyalash amalga oshiriladi: SQL in’yektsiyasi, CRLF in’yektsiyasi, saytlararo skript, bufer to‘lib toshishi va boshqalar.

3. Tasodifiy so‘rovlar, bunda so‘rovlar parametrlarning tasodifiy generatsiyalanib uzatilishi bilan tasodifiy hosil bo'ladi (qo‘shimcha parametrlar qo‘shish ham mumkin) yoki oldindan toifalashtirilgan parametrlarni tasodifiy o‘zgartirish (masalan, telefon raqami maydonida harflarni o‘tkazish). CSIC 2010 HTTP so‘rovini kiritish xususiyatlarining to‘liq ro‘yxati quyidagi jadvalda keltirilgan [8].

2.5 jadval

CSIC 2010 HTTP so‘rovlar yozuvlarining xususiyatlari

Xususiyat	Tavsifi	Xususiyat	Tavsifi
1. *index*	paket raqami(unikal emas)	10. *protocol*	Ulanishni amalga oshirish protokoli turi
2. *method*	parametrlarni uzatish usuli (*GET, POST*)	11. *userAgent*	so‘rov yuborilgan protokol nomi
3. *url*	GET parametrlari bilan birga URL manzili so‘rovi	12. *pragma*	keshlash xususiyati
4. *cacheControl*	request so‘rovda keshning mavjudligi	13. *accept*	hujjat turi, uning xususiyatlari

5. *acceptEncoding*	so‘rovni kodlash	14. *acceptCharset*	kodlash turi
6. *acceptLanguage*	so‘rov tili	15. *host*	ulanish xost nomi
7. *connection*	ulanish turi	16. *contentLength*	barcha xususiyatlar bilan so‘rov uzunligi
8. *contentType*	so‘ralgan kontent turi	17. *cookie*	cookie fayl tarkibi
9. *payload*	uzatiluvchi request parametrlar	18. *label*	yorliq (anomal yoki anomal bo‘lmagan so‘rov)

Shunday qilib, CSIC 2010 HTTP da ma’lumotlar to‘plami uchun formal so‘rov modeli 18 o‘lchovli vektor hisoblanadi.

Enron Dataset ma’lumotlar to‘plami

Standartlar ro'yxatiga (RFC822, RFC2142, RFC2368, RFC5322, RFC2045) muvofiq minglab avtomatik ravishda yaratilgan SMTP so‘rovlarini o‘z ichiga olgan SMTP protokoli uchun ma’lumotlar to‘plami. Ushbu to‘plam SMTP protokoli yordamida Mail-serverlari orqali suqulib kirishni aniqlash tizimlarini sinab ko‘rish uchun ishlatiladi. To‘plam Internet tarmog‘idagi elektron xabarlar serveri ishlashining bir qismi sifatida kelgan SMTP serveriga so‘rovlarni taqlid qiladi. Enron Dataset ma’lumotlar to‘plami tarkibi quyidagi jadvalda keltirilgan [9].

2.6-jadval

Enron Dataset ma’lumotlar to‘plami

№	To‘plamning nomi	Yozuvlar soni	Tavsifi
1.	*Spam*	50987	Anomal so‘rovlar to‘plami
2.	*Ham*	189523	Test so‘rovlar to‘plami
3.	*Raw dataset*	319264	Anomal va test so‘rovlarining to‘liq

			to‘plami (odatiy trafik)

Barcha SMTP so‘rovlari anomal va anomal emas deb belgilangan.

Anomal so‘rovlar quyidagilarni o‘z ichiga oladi:

- lotin bo‘lmagan kodlashdagi xabarlar;
- virus tanasi biriktirilgan xabar;
- soxta sarlavhali xabarlar;
- ko‘plab xususiyat qiymatlari bo‘lgan xabarlar;
- *XSS* xujumlar;
- soxta yuboriladigan parametrlarga ega xabarlar.

Barcha xabarlar Raw (xom) formatida taqdim etiladi. Bundan tashqari, barcha xabarlar ikkita to‘plamda saqlanadi: Raw va Processed. "Raw" da “Preprocessed”dan ko‘ra ko‘proq xabarlar mavjud, chunki:

1. dastlab, xabarlar boshlang‘ich holatda saqlanadi va shundan keyingina qayta ishlanadi;

2. oldindan ishlov berish jarayonida spam-xabarlar yoki xavfli xabarlar spam koeffitsientlarini keyingi aniqlash uchun tasodifiy tanlab olinadi.

Enron Dataset ma’lumotlar to‘plami maydonlarning to‘liq ro‘yxati 2.7-jadvalda ko‘rsatilgan

2.7-jadval

Enron Dataset so‘rovlar yozuvlarining xususiyatlari

Xususiyat	Tavsifi	Xususiyat	Tavsifi
1.Return-Path (RFC 821, RFC 1123)	xabarni belgilangan manzilga yetkazishning iloji bo‘lmagan taqdirda qaytarish manzili. MAIL FROM va From:, Sender: yoki	*9.To (RFC 822, RFC 1123)*	Qabul qiluvchining ismi va manzili. U bir necha marta bo‘lishi mumkin (agar xabar bir nechta qabul qiluvchilarga qaratilgan bo‘lsa). Ushbu maydon asosida SMTP

	Reply-To sarlavhalaridan farq qilishi mumkin, lekin odatda MAIL FROM bilan mos keladi		RCPT TO maydonining mazmuni shakllanadi.
2.Received (RFC 822, RFC 1123)	xabarning har bir aniq pochta serveri (MTA) orqali o‘tishi haqidagi ma’lumotlar. Bir nechta pochta serverlaridan o‘tishda (odatiy holat) oldingi sarlavhalar ustiga yangi sarlavhalar qo‘shiladi, natijada ko‘chirish jurnali teskari tartibda (eng yaqin qabul qiluvchidan eng uzog’iga)	*10.MIME-Version (RFC 1521)*	ushbu xabar yaratilgan MIME versiyasi. Ko‘pincha bu nom boshqalardan oldin yaratiladi, shuning uchun u odatda birinchi (ya’ni ro‘yxatdagi oxirgi) bo‘ladi.
3.From (RFC 822, RFC 1123, RFC 1036)	yuboruvchining nomi va manzili (aynan shu sarlavhada yuboruvchining nomi yozilgan matn maydoni paydo bo‘ladi). Return-pathga mos kelmasligi va hatto SMTP MAIL FROM sarlavhasiga	*11.Sender(RFC 822, RFC 1123)*	Xabar yuboruvchi. Kimningdir (from) nomidan xabar boshqa shaxs tomonidan yuborilganligini bildira olish uchun qo‘shilgan (masalan, boshliq nomidan kotib). Ba’zi pochta mijozlari xabarni sender va from huzurida

	mos kelmasligi mumkin:		ko‘rsatadi.. Sender axborot sarlavhasi xisoblanadi (shuningdek, sarlavhadan farq qilishi mumkin SMTP MAIL FROM)
4.Cc (RFC 822, RFC 1123)	(inglizcha carbon copy) nusxasi yuborilgan xabarni ikkinchi darajali qabul qiluvchilarning ismlari va manzillarini o‘z ichiga oladi. SMTP RCPT TO maydonini, shuningdek, "To" maydonini shakllantirishda ishtirok etadi	*12.Bcc (RFC 822, RFC 1123)*	(inglizcha blind carbon copy) boshqa qabul qiluvchilarga ko‘rsatilmasligi kerak bo‘lgan elektron pochta qabul qiluvchilarining ismlari va manzillarini o‘z ichiga oladi. "To" va SMTP RCPT TO kabi maydonini shakllantirishda ishtirok etadi "cc" lekin yuborilayotgan xabarda emas
5.Reply-To:(RFC 822, RFC 1036)	ushbu xabarga javob beradigan ism va manzil ko‘rsatilishi kerak. Agar, masalan, xabar robot tomonidan yuborilsa, u holda Reply-To pochta qutisining xabarga javob qabul qilishga	*13.Message-ID (RFC 822, RFC 1036)*	unikal xabar identifikatori

	tayyor manzili bo‘ladi.		
6.In-Reply-To(RFC 822)	bu xabar javob bo‘lgan Message-IDni ko‘rsatadi (bundan foydalanib, pochta mijozlari yozishmalar zanjirini osongina qurishlari mumkin - har bir yangi javob oldingisining Message-ID sini o‘z ichiga oladi.)	*14.Subject(RFC 822, RFC 1036)*	xabar mavzusi
7.Date(RFC 822, RFC 1123, RFC 1036)	xat yuborish sanasi	*15.Content-Type(RFC 1049, RFC 1123, RFC 1521, RFC 1766)*	elektron pochta mazmuni turi (HTML, RTF, Plain text) va elektron pochta yaratilgan kodlash (kodlash haqida quyida)
8.Return-Receipt-To (RFC 2076)	Qabul qiluvchining pochta serveri yetkazib berish haqida bildirishnoma yuborishi kerak bo‘lgan E-Mail.B RFC 2076 "Not internet standard" bo‘limida keltirilgan,	*16.Disposition NotificationT: (RFC 3798)*	E-Mail, agar foydalanuvchi ruxsat bergan bo‘lsa, qabul qiluvchining elektron pochta mijozi yetkazib berish xabarnomasini yuborishi kerak (sozlamalar va boshqalar orqali).

	shuning uchun serverlar tomonidan qo‘llab-quvvatlanmasligi mumkin		
		17. Xparametrlar	"X-" bilan boshlanadigan pochta mijozlari, serverlari va robotlarining shaxsiy sarlavhalari (masalan, X-Mailer, X-MyServer-Note-OK yoki X-Spamassasin-Level)

Shunday qilib, Enron Dataset ma’lumotlar to‘plami uchun formal so‘rov modeli 17 o‘lchovli vektordir.

2.2 Sun’iy immun tizimi va unga qo‘yiladigan talablar

Suqulib kirishlarni aniqlash tizimlarini rivojlantirishning yangi yo‘nalishidan biri sun’iy immun tizimlari (SIT) asosida adaptiv algoritmlarni ishlab chiqish hisoblanadi. Ushbu ishda tavsiya etilgan mashinali o‘qitish modellaridan biri sun’iy immun tizimiga (SIT) asoslangan model sanaladi. Uning funksional va dasturiy qo‘shimchalarini tavsiflashdan oldin, asosiy talablarni shakllantirish zarur, ularning bajarilishi tizim samaradorligining zarur darajasini ta’minlashga imkon beradi.

Sun’iy immun tizimiga qo‘yiladigan talablar

Sun’iy immun tizimi uchun umumlashtirilgan tamoyillardan kelib chiqqan holda to‘plamlarni tasniflash muammosini hal qilishni amalga oshiradigan sun’iy immun tizimi quyida keltirilgan talablarga javob berishi kerak:

- *Tahlil qilinadigan ob'yektlarni saqlash*. Tasniflashning vazifasi ma'lumotlarni saqlashning yagona formatini nazarda tutadi, uning asosida sun'iy immun tizimlari o'qitiladi, hamda uni keyinchalik ishga tushiriladi.

- *Ma'lumotlar unifikatsiyasi***.** Axborot almashish va uzatish tizimlarining ko'p turlari mavjud. Loyihalashtiriladigan sun'iy immun tizimi uchun tahlil qilinadigan format turini farqi bo'lmasligi lozim: TCP protokoli orqali yoki HTTP protokoli orqali kelgan ma'lumotlar bloki bo'lishidan qat'iy nazar.

- *Ma'lumotlarni qayta ishlashning ko'lami***.** Loyihalashtirilgan tizim kichik hajmdagi ma'lumotlarni ham, ularning massivlarini ham teng darajada qayta ishlashi kerak. Ekvivalentlik qayta ishlash tamoyillaridagi bir xillikni anglatadi.

- *Tuzilmaviy ko'lamlik***.** Sun'iy immun tizimini tashkil etuvchi ko'p sonli elementlarning mavjudligi butun axborot tizimi va xususan suqulib kirishni aniqlash tizimi doirasida hisoblashlarni parallellashtirish muammosini hal qilishni nazarda tutadi.

- *Shovqinlarga bardoshlilik***.** Sun'iy immun tizimi tahlil qilinadigan ob'yektlardan foydali belgilarni (xususiyatlarni) sifatli ajratib olishi va belgilangan vazifalar bo'yicha ma'lumotlarni samarali tasniflashi lozim.

Yuqorida tavsiflangan talablar sun'iy immun tizimini loyihalashni tashkil etishda nazariy asoslarni hosil etadi. Sun'iy immun tizimining elementlari ko'rib chiqilgan [10].

2.3 Sun'iy immun tizimining elementlari

Sun'iy immun tizimlarida axborot sinflari - bu sun'iy immun hujayralari ko'payish to'plamlari hisoblanadi.

Sun'iy immun tizimlar nazariyasida tadqiq etilayotgan to'plamning elementi (ob'yekti) sifatida B-hujayralar (β-hujayralar, keyinchalik β-element) tushunchasi ajratiladi. B-hujayraning eng xarakterli ko'rinishi vektor hisoblanadi, lekin elementni, matritsa ko'rinishida ham berish mumkin. Bundan tashqari o'z tuzulmasida tadqiq etilayotgan to'plamning barqaror yechimi elementi mavjud element (ob'yekt) sifatida xotiraga ega B-hujayra tushunchasi (β^m-hujayra, β^m-

hujayra, keyin β^m-element) ajratiladi. Barqaror yechim deyilganda, vektor atributlarining muvaffaqiyatli kombinatsiyasini tushunish mumkin. β^m-elementlar to‘plami G ning gen kutubxonasi deb ataladi. Umumiy tasavvurga ko‘ra, β^m-elementlar soni har β-elementlar sonidan doimiy ravishda kam bo‘ladi. β-elementlar va β^m-elementlarning nisbati ko‘rilayotgan masalaga qarab turlicha bo‘ladi, ko‘pincha 20-30% ni tashkil etadi va empirik usulda topiladi. Har qanday sun’iy immun tizimining yakuniy maqsadi testlash bosqichida birinchi va ikkinchi darajali xatolarni minimallashtiradigan gen kutubxonasini yaratish hisoblanadi.

Shunday qilib, har qanday W sun’iy immun tizimi β va β^m elementlar to‘plamini o‘zida aks ettiradi, $W = B\ U\ B^m = (\beta_1 \dots \beta_k) U (\beta_1^m \dots \beta_s^m)$.

Ushbu ishda β -element dublet $\beta = (c, P)$ ni aks ettiradi, bu yerda $c \in N$ hujayra sinfi, $P = (p_1 \dots p_n) \in R^n$ - n o‘lchovli Evklid fazosidagi $||p|| <= 1$ birlik gipersfera ichida yotgan vektor. Faqat anomal so‘rovlarni aniqlash maqsadida c sinf qiymati har doim aniq bo‘ladi va birlik tahdidni aniqlaydi (anomal so‘rovlar sinfi).

β-elementlar uchun ko‘rsatkichlar

Sun’iy immun tizimlarida ko‘rsatkich sifatida Affinlik ($Affinity$ yoki α) tushunchasi ishlatiladi. Ikki elementning affinligi – bu elementlarni tashkil etuvchi umumiy obyektlar sonini norma orasidagi nisbati. Ikki element normasi - har bir elementni tashkil etuvchi obyektlarning minimal soni. Boshqacha qilib aytganda, sun’iy immun tizimlarida affinlik elementlar orasidagi masofaning qiymati hisoblanadi.

- β_i - element β_j -elementni “taniydi” agar ikkala element ham bir sinfga tegishli bo‘lsa va ular orasidagi masofa chegaraviy qiymat $Affinity(\beta_i, \beta_j) \leq AT$ dan kichik yoki unga teng bo‘lsa (affinlik chegarasi AT-*Affinity Threshold*).

Ushbu ishda tuzilgan ko‘rsatkichli fazoning mavjudligi sababli masofa formulasini ko‘rsatkich sifatida ishlatish taklif etilgan.

AT sifatida, klaster elementlari va yolg‘on markazlar orasidagi o‘rtaarifmetik masofadan foydalanish taklif etilgan. AT koeffitsientini hisoblashda elementlar

soni birga teng bo‘lgan klasterlar olinmaydi, bunday hollarda element klasterning markazi hisoblanadi.

AT parametri bilan ishlashda W immun tarmog‘ining holati uchun ikkita qoida mavjud:

- Apoptoz – agar V_i xujayrasi V_j xujayrasini «tanisa», u holda V_i xujayra W dan o‘chiriladi;
- Immunizatsiya - agar V_i, W immun tarmog‘ining barcha boshqa hujayralariga qaraganda V_j ga yaqinroq bo‘lsa, V_i to‘plami W qo‘shiladi.

Ya’ni, har bir β-element atrofida AT radius maydon hosil bo‘ladi, unda uchbu maydonga kiruvchi barcha elementlar (bloklar) anomal, qolgan elementlar esa anomal bo‘lmagan deb hisoblanadi. Affinlik qiymati barcha β-elementlar uchun bir xil ko‘rsatilganligini hisobga olib, bir xil AT radiusli “sharlar” bilan ishlanadi.

Sun’iy immun tizimidagi operatsiyalar

Algoritmning o‘zgaruvchanligini saqlab qolish va yangi β-elementlar sonini ko‘paytirish maqsadida sun’iy immun tizimida mutatsiya *(Mutating)* va klonlash *(Cloning)* operatsiyalari mavjud. Elementning mutatsiyasi deganda uning ba’zi atributlar qism qiymatlarini tasodifiy o‘zgartirish jarayoni tushuniladi. Mutatsiya koeffitsienti o‘zgartirilishi kerak bo‘lgan umumiy atributlar sonini ko‘rsatadigan qiymat tushunilgan. Boshqacha qilib aytganda, Mutatsiya operatsiyasi(*Mutating*) funksiya ko‘rinishida aniqlanadi:

$$Mutating\big(\beta = (\beta_1, \dots, \beta_n)\big) = \big(\beta_1, \dots, \beta'_{i_1}, \dots, \beta'_{i_k}, \dots, \beta_n\big),$$

$$k = \lfloor \varepsilon \cdot n \rfloor, \varepsilon \in [0,1],$$

β'_i – bu yerda β –o‘zgartiriladigan element vektorning k atributlari, e - mutatsiya koeffitsienti.

Anomal so‘rovlar uchun ε ni boshlang‘ich qiymati sifatida quyidagi formulani qo‘llash mumkin:

$$\varepsilon = 1 - \frac{1}{\vartheta}$$

ϑ - bu yerda so‘rov obyekti doirasidagi atributlar soni. Ushbu formulada so‘rov vektorining kamida bitta atributi o‘zgarishga uchraydi.

Klonlash operatsiyasi (*Cloning*) β - elementlarni oddiy elementni ketma-ket “nusxalash” funktsiyasi tushuniladi. U mutatsiya operatsiyasidan so‘ng qo‘llaniladi va mavjud elementlar to‘plamida yangi olingan β - elementlarning dublikatlarini yaratishga qaratilgan. Amaliy jihatdan amalga oshirish nuqtai nazaridan klonlash operatsiyasi kompyuter operativ xotirasida β-element obyektining virtual nusxasini yaratishni anglatadi.

Shunday qilib, mutatsiya operatsiyasi yangi anomal so‘rovlarni tanib olish qobiliyatiga ega bo‘lgan yangi elementlarning yaratilishini ta’minlaydi, klonlash esa ularning tizim ichida “tarqalishi” uchun qo‘llaniladi. Doimiy ravishda yangi β-elementlarning yaratilishi va ularni boshqa elementlargacha bo‘lgan masofa orqali yo‘q qilishning mavjud mexanizmi tizimga dinamiklik va variativlik hususiyatini beradi. Tahdidlarni aniqlash jarayonida o‘zini tavsiya etgan elementlarni kelgusida yaratish maqsadida klonlash va mutatsiya faqat β^m – elementlari ustida amalga oshiriladi.

Shunday qilib, β-elementlar va β^m-elementlarni muvozanatlash mexanizmi mavjud. β-element uchun fiksirlangan qiymat bilan mutatsiya va klonlash operatsiyalarini qo‘llashda β^m-elementlar sonining β-elementlarga bog‘liqligi haqidagi ta’rif isbotlanadi.

SITda tashqi ta’sir mexanizmi

Tashqi ta’sir mexanizmi deganda so’rovni tasniflash bosqichida algoritmning ishlashini kuzatish imkonini beruvchi asinxron mexanizm tushuniladi. U operator yoki tashqi ekspert tizimining harakatlarini ifodalaydi.

Tizimning ishlashi doimiy xarakterga ega bo‘lganligi sababli, o‘z-o‘zini o‘qitish va o‘z-o‘zini tartibga solish jarayoni ham ish vaqti bilan to‘xtatilmaydi. Kiruvchi so‘rovlar bo‘yicha anomal va anomal bo‘lmagan sinflarga keyingi tasniflashda tizim tomonidan tahlil va qaror aniqligi, qabul qilinganlarning soniga mutanosib ravishda oshishi lozim.

Yuqorida tavsiflangan algoritmga qo‘shimcha ravishda, sun’iy immun

tizimining ishlashini tshkil etuvchi uchun bir qator xarakterli parametrlarni belgilash kerak [11].

Sun'iy immun tizimining formal amalga oshirilishining tavsifi

Sun'iy immun tizimiga asoslangan tasniflash algoritmini quyidagi bosqichlarga bo'lish mumkin.

O'qitish bosqichi:

1. Algoritmni ishga tushirish (boshlang'ich parametr va konstantalarni topshirish)
2. Muvofiqlikni tahlil qilish mexanizmi orqali β^m-elementlar to'plamini shakllantirish;
3. O'qitish jarayonida mutatsiya va klonlash operatsiyalari orqali ularning "xilma-xilligini" oshirish;
4. Apoptoz;
5. Immunlash;
6. Tasniflashning chegaraviy qiymatini belgilash yordamida natijalarni tuzatish;
7. 3-6-bosqichlarni boshqa qiymatlar bilan takrorlash;
8. Tanlangan ma'lumotlar to'plamiga nisbatan eng mos natijalarga ega SITni tanlash.

Tasniflash bosqichi:

1. Atributlar kirish obyektinining normallashtirilgan ikkilik ko'rinish bilan SITning β -elementlar fazosiga akslantirish;
2. Muvofiqlik tahlili mexanizmining masofa funktsiyasi orqali eng yaqin β^m-elementni aniqlash;
3. Kirish tasvirining eng yaqin elementiga sinf belgilash (anomal yoki anomal bo'lmagan so'rov).

Sun'iy immun tizimi konstantalari

Sun'iy immun tizimi algoritmining funktsional qismini tavsiflash uchun bir qator konstantalar aniqlangan:

- TK - mustaqil β -elementlar to'plami. Algoritm boshida TK to'plami

bo‘sh bo‘ladi.

- KP - β^m-elementlar to‘plami. Algoritm boshida KP to‘plami bo‘sh bo‘ladi.

- TKP - SIT algoritmini tayyorlash jarayonida foydalaniladigan β^m-elementlar soni.

- UK - SIT algoritmida klonlash darajasi uchun javob beradigan konstanta.

- UM - SIT algoritmidagi mutatsiya darajasi uchun javob beradigan konstanta.

- PA – affinlik chegaraviy qiymati (ushbu qiymatdan oshib ketishi, masofa hisoblanayotgan ikkita vektorning ekvivalent emasligini anglatadi). AT qiymati affinlik chegarasining qiymati sifatida olinadi - klaster elementlari va yolg‘on markazlar orasidagi o‘rtacha arifmetik masofa.

Sun’iy immun tizimini amalga oshirish

Sun’iy immun tizimi algoritmini amaliy amalga oshirishni ko‘rib chiqamiz. Yuqorida aytib o‘tilganidek: algoritmning ishi to‘rt bosqichga bo‘lingan: initsializatsiya, o‘qitish, tayyorlash va tasniflash.

Sun’iy immun tizimining umumiy dasturi quyida keltirilgan:

Dastur ishga tushirilishida, ishga tushirish protsedurasidan so‘ng (initializatsiya muolajasi), o‘qitish jarayoni (tizimni o‘qitish muolajasi) va tayyorlov jarayoni (tizimni tayyorlov muolajasi) boshlanadi.

Tayyorlov jarayonining vazifasi β -elementlar vektorlaridan foydalangan holda yangi tahdid shablonlari G' gen kutubxonasini shakllantirish. Tizimni o‘qitish va tizimni tayyorlov jarayoni muolajalari dastlabki β -elementlarni, β^m -elementlarni yaratishni, shuningdek, populyatsiyani yangilash muolajasidan foydalangan holda ularga klonlash va mutatsiya usullarini qo‘llashni ko‘zda tutgan. Tizimning o‘qitish muolajasiga kirishiga ma’lum muvofiqlik tahlil qilish usuli bilan olingan G gen kutubxonasi (KP to‘plamini tashkil qiladi) va G to‘plam vektorlarni hisobga olmagan holda o‘qitish to‘plamining anomal so‘rovlarining M vektorlari to‘plami uzatiladi. (TK to‘plamini tashkil qiladi).

Amalga oshirish mexanizmi doirasida tizimni o‘qitish muolajasi.

O‘qitish muolajasi bajarib bo‘linganidan so‘ng, tizim kiruvchi ma’lumotlarning noma’lum bloklarini (masalan, ma’lumotlar to‘plamidan so‘rovlar) tasniflashga tayyor bo‘ladi [10].

So‘rovlarni tasniflash uchun tuzilishi bo‘yicha β -elementga o‘xshash vektor (AG) yaratiladi. Berilgan so‘rovning anomal yoki anomal bo‘lmagan so‘rovlar sinfiga munosabatini aniqlash uchun tasniflash protsedurasi (*classifyMessage* protsedurasi) qo‘llaniladi:

Algoritmni o‘qitish va undan keyingi ishlash jarayonida tizim bo‘yicha to‘plangan bilimlarga tasniflash jarayonini akslantirish zarurligi sababli, quyidagi formal amalga oshirishga ega bo‘lgan populatsiyani yangilash kabi protsedura joriy etilgan:

Algoritmning variativligi va dinamikligini ta’minlash uchun klonlash va mutatsiya protseduralari qo‘llaniladi (CloneMutation umumiy protsedurasi). Berilganidan kichik bo‘lgan eng katta butun sonni ajratish klonlangan hamda mutatsiyaga uchragan elementlarning sonini aniqlaydigan quyi chegaraviy qiymat.

2-bob bo‘yicha xulosa

Magistrlik dissertatsiya ishining ikkinchi bobida anomaliyalarni aniqlash tizimlarini o‘qitish va testlash bosqichlarida qo‘llaniladigan ma’lumotlar to‘plami ko‘rib chiqildi, quyidagi natijalar olindi:

- mashinali o‘qitish tizimlarini o‘qitish va sinovdan o‘tkazishda qo‘llaniladigan ma’lumotlar to‘plamlari NSL-KDD ISCX Dataset, CSIC 2010 Dataset, Enron Dataset tadqiq va tahlil qilindi ;

- tarmoqni himoyalashda suqulib kirishlarni aniqlash tizimlarini loyihalashda qo‘llaniladigan sun’iy immun tizimi tuzilmasi va unga qo‘yiladigan talablar ko‘rib chiqildi;

- sun’iy immun tizimiga asoslangan suqulib kirishlarni aniqlash tizimlarini loyihalashda qo‘llaniladigan elementlar tadqiq qilindi.

3 BOB. SUN’IY IMMUN TIZIMIGA ASOSLANGAN ANOMAL SO‘ROVLARNI ANIQLASH TIZIMINI LOYIHALASH

3.1 Su’niy immun tizimiga asoslangan anomaliyalarni aniqlash tizimi arxitekturasi va algoritmi

Suqilib kirishlarni aniqlash tizimining arxitekturasi tegishli mantiqiy elementlar va ularning ishlash bosqichlaridan iborat blokli tuzilma ko‘rinishga ega. Quyidagi rasmda yuqorida taklif qilingan usullar va algoritmlarni amalga oshiradigan anomal so‘rovlarni o‘qitish va tasniflash uchun quyi tizimning ishlash arxitekturasi ko‘rsatilgan.

So‘rovlarni kiritish quyi tizimi - kirish parametrlarini keyinchalik kompleksning asosiy qismiga o‘tkazish uchun qabul qilishni amalga oshiruvchi modul.

So‘rovlarni parametrlash bloki - yuqorida keltirilgan metodologiyaga muvofiq so‘rovni parametrlashtirilgan chiqishga keltiriladigan modul.

O‘qitish bloki - yondashuv asosida sun’iy immun tizimini o‘qitishni amalga oshirish moduli.

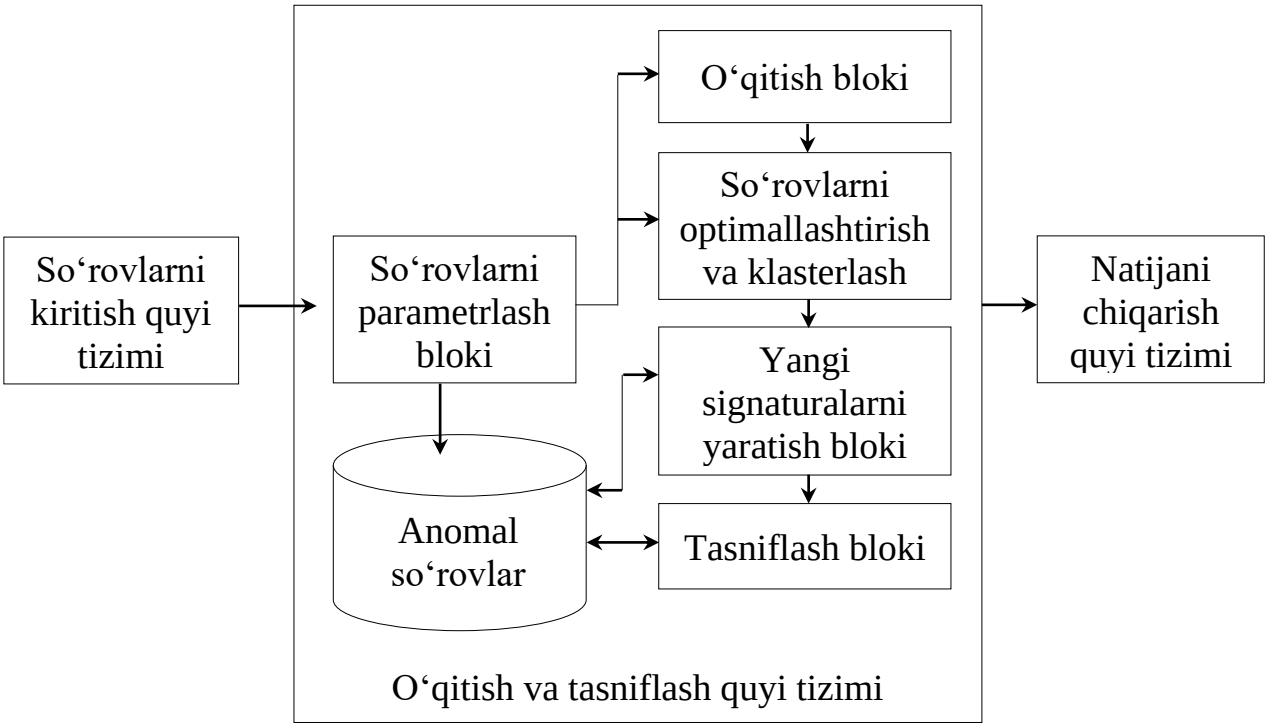
So‘rovlarni optimallashtirish va klasterlash bloki – so‘rovlarni optimal shaklga keltirish, so‘ngra belgilangan mezonga muvofiq klasterlash.

Yangi signaturalarni yaratish bloki – ma’lumotlar to‘plamida mavjud bo‘lmagan yangi signaturalarni yaratishni amalga oshiruvchi sun’iy immun tizimining komponenti

Tasniflash bloki - so‘rovlar sinfiga anomal/anomal bo‘lmagan so‘rov belgisini tayinlangan holda tasniflash bosqichi.

Natijani chiqarish quyi tizimi - sun’iy immun tizimi natijalarini chiqarish moduli.

Yuqorida tavsiflangan bloklar va quyi tizimlarni yagona kompleksga birlashtirish uchun sun’iy immun tizimiga asoslangan suqilib kirishlarni aniqlash tizimi dasturiy ta’minotining ishlash sxemasi [12].



3.1 - rasm. Anomal so‘rovlarni o‘qitish va aniqlash quyi tizim arxitekturasi

Tizim tuzilmasi - modellarning tavsiflari to‘plami bo‘lib, bu yerda har bir model mashinali o‘qitish texnologiyasini (jumladan, tavsiya etilgan sun’iy immun tizimini) dasturiy amalga oshirilishi.

O‘qitish bosqichida - so‘rovlar hisobiga algoritmni o‘qitish amalga oshiriladi. O‘qitish misollari to‘plamidan tashqari, ushbu komponent kirishga model tavsiflari to‘plami uzatiladi, shundan so‘ng u har bir tanlangan model uchun o‘qitish jarayoni bajariladi.

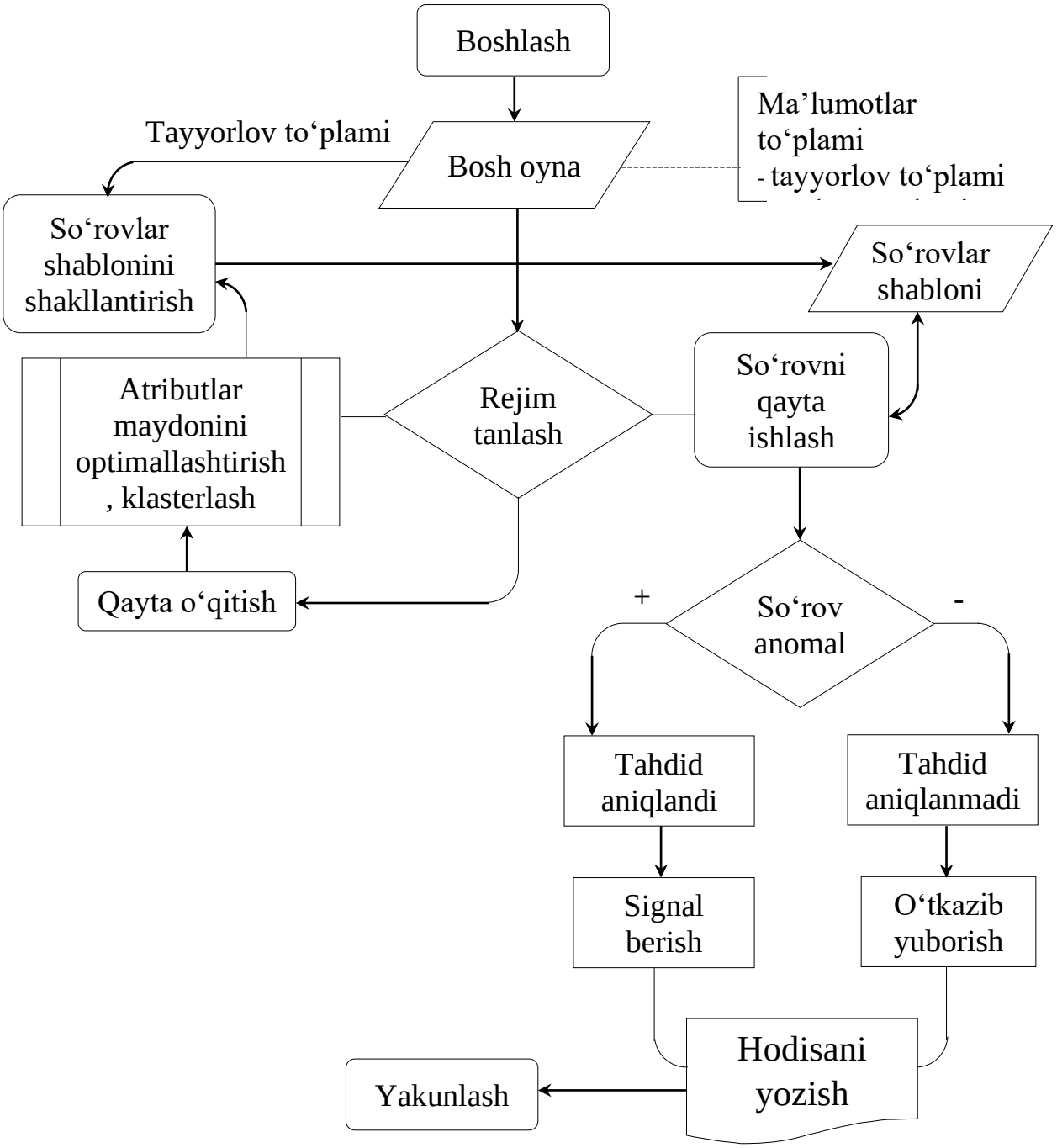
Modellar to‘plami - o‘qitish natijasida olingan tasniflash algoritmlarining dasturiy amalga oshirilishi. O‘qitish tanlanmasida mavjud bo‘lmagan so‘rovlar to‘plami kirishga uzatiladi.

Korrelyatsiya bosqichi - samarali moslashuvchan modelni tanlash amalga oshiriladi. Ushbu bosqichning natijasi eng yaxshi ko‘rsatkichga ega bo‘lgan model, to‘g‘ri tasniflangan misollar ma’lumotlar bazasiga joylashtiriladi.

Taklif etilgan tizim ikkita rejimda ishlaydi - o‘qitish va tasniflash.

Birinchi holatda, taklif qilingan ma’lumotlar to‘plamlari bo‘yicha bir nechta modellarni o‘qitilishi amalga oshiriladi, ikkinchi holatda, tizimning to‘g‘ri ishlashini tekshiradigan so‘rovlar tahlili. Tizimning ishlashi natijasi yakuniy

mashinali o‘qitish modeli hisoblanadi, o‘qitish tanlanmasiga kiritilmagan misollarni tahlil qilishda eng yaxshi natijalarni ko‘rsatadi - ushbu vazifani korrelyatsiya bloki amalga oshiradi.



3.2 - rasm. SIT ga asoslangan hujumni aniqlash tizimi algoritmi

O‘qitish va testlash formal algoritmi quyidagi qadamlar ketma-ketligiga ega:

1 - qadam. Tadqiq qilingan so‘rovlar to‘plami olinadi, ikkita kichik to‘plamga (namunalarga) bo‘linadi: o‘qitish va test.

2 - qadam. So‘rovlar kortejlari atributlar fazosi bilan shakllantiriladi.

3 - qadam. Kortejlarni binarlash va ulardan to‘g‘ri burchakli A matritsani yaratish.

4 - qadam. Singulyar bo‘lish usulidan foydalanib, 3 - bosqichda olingan ma’lumotlardan iborat bo‘lgan A matritsasi olinadi, atributlarning muhim kombinatsiyalari shakllantiriladi.

5 - qadam. Muhim atributlar ajratiladi, klaster markazlarini alohida to‘plamga (G gen kutubxonasi) ajratgan holda so‘rovlarni klasterlash jarayoni amalga oshiriladi.

6 - qadam. 5 - bosqichda olingan so‘rovlar to‘plami va sun’iy immun tizimi yordamida anomal so‘rovlarning yangi to‘plami (G' to'plami) hosil qilinadi.

7 - qadam. Singulyar taqsimlashni teskari akslantirishdan, shuningdek round yaxlitlash usulidan foydalanib, xususiyatlarning atribut fazosidan G va G' to‘plamlarning elementlari boshlang‘ich atributli (1-qadam kabi) anomal so‘rovlarga almashtiriladi.

8 - qadam. Anomal so‘rovlarining test to‘plamidan foydalanib, algoritmning ishlash samaradorligi baholanadi.

Su’niy immun tizimlarining tashqi ta’sir mexanizmini (keyingi qayta o‘qitish uchun o‘quv namunasiga yangi anomal so‘rovlarni kiritish) amalga oshirish uchun algoritmning qisqartirilgan versiyasi taklif etilgan [13].

Tanlangan ma’lumotlar to‘plamlaridan tashqari (NSL-KDD DataSet, CSIC 2010, Enron Dataset), mijoz-server modeli doirasida suqulib kirishni aniqlash tizimi tanlangan yondashuvning to‘g‘riligini tekshirish uchun korporativ tizim uchun belgilangan arxitektura qo’llanilgan.

Tahlil qilinadigan ma’lumotlar sifatida CSIC 2010 va Enron Dataset so‘rovlariga o‘xshash tuzilishga ega so‘rovlar tadqiq qilingan, bu yerda korporativ portalning (CP) veb-server va pochta serveri himoyalangan obyekt sifatida olingan.

Mashinali o‘qitish algoritmlari sifatida taklif qilingan algoritmlar ko‘rib chiqilgan: mantiqiy regressiya va sun‘iy neyron tarmoqqa asoslangan algoritm. Ushbu algoritmlarni tanlash hujumlarni aniqlash tizimlarida keng qo‘llanilishi bilan bog‘liq.

3.2 Mashinali o‘qitishga asoslangan anomaliyalarni aniqlash mexanizmi samaradorligini tahlil qilish

Mashinali o‘qitish tizimi ishlash jarayoni samaradorligini baholash uchun, birinchidan, tizim faoliyatining u yoki bu jihatini miqdoriy tavsiflovchi ko‘rsatkichlar to‘plamini aniqlash, ikkinchidan, natijaga erishish uchun statistik ahamiyatga ega tajriba o‘tkazish tartibini ishlab chiqish kerak. Asosiy samaradorlik ko‘rsatkichlari sifatida ikki turdagi xatoliklar aniqlanadi:

- Birinchi turdagi xatolar (yolg‘on ishga tushish xatoliklari, *false negative, FN*) – anomal bo‘lgan so‘rovlar, algoritm yordamida noto‘g‘ri tasniflangan anomal bo‘lmagan so‘rovlar (tahdidni o‘tkazib yuborish va algoritmni yetarlicha to‘liq emasligi);
- Ikkinchi turdagi xatolar (hodisani o‘tkazib yuborish xatoliklari, *false positive, FP*) - anomal bo‘lmagan so‘rovlar, algoritm yordamida noto‘g‘ri tasniflangan anomal bo‘lgan so‘rovlar deb (usulning yolg‘on tasnifi yoki aniqligi).

Ushbu ko‘rsatkichlarning formal ta’rifini keltiramiz, tushunchalarning aniqligi uchun anomal so‘rovlarni aniqlash muammosiga aloqador ta’riflar keltiriladi. Quyidagi tushunchalar kiritiladi:

- ijobiy signal – tahlil qilinayotgan so‘rovning anomal hodisa ekanligini ko‘rsatuvchi suqilib kirishlarni aniqlash tizimining javobi;
- salbiy signal - tahlil qilinayotgan so‘rovning anomal hodisa emasligini ko‘rsatuvchi suqilib kirishlarni aniqlash tizimining javobi.

Har qanday IDS (suqilib kirishlarni aniqlash tizimi)ning javobi to‘rtta sinfdan biriga ajratish mumkin:

1) haqiqiy ijobiy signal (*true positive, TP*) – to‘g‘ri tasniflangan anomal so‘rovlar;

2) yolg‘on ijobiy signal (*false positive, FP*) - tizim anomal bo‘lmagan so‘rovni anomal so‘rov deb noto‘g‘ri aniqlashi;

3) haqiqiy salbiy signal (*true negative, TN*) – to‘g‘ri tasniflangan anomal bo‘lmagan so‘rovlar;

4) yolg‘on salbiy signal (*false negative*, *FN*) - tizim anomal so‘rovni anomal bo‘lmagan so‘rov deb noto‘g‘ri aniqlashi (3.1-jadval).

3.1-jadval

IDS signallarining turlari

	Anomal bo‘lgan so‘rov	Anomal bo‘lmagan so‘rov
Ijobiy signal	*TP*	*FP*
Salbiy signal	*FN*	*TN*

Suqilib kirishlarni aniqlash tizimini samaradorligini noto‘g‘ri ijobiy va noto‘g‘ri salbiy signallar darajalarini o‘lchash yo‘li bilan eksperimental baholash mumkin (R_k - signalning k-turidagi signal darajasi, N_l - eksperimentdagi l-turidagi signallar soni, $k, l\ c\{TP, FP, TN, FN\}$):

haqiqiy ijobiy signallar darajasi nisbat bilan belgilanadi:

$$R_{TP} = \frac{N_{TP}}{N_{TP} + N_{FN}}$$

noto‘g‘ri ijobiy signallar darajasi nisbatda aniqlanadi:

$$R_{FP} = \frac{N_{FP}}{N_{FP} + N_{TN}}$$

Suqilib kirishlarni aniqlash tizimida tez-tez ishlatiladigan xarakteristikalardan biri $R_{TP} = f(R_{FP})$ funktsiyasini ifodalovchi ROC egri chizig'i (receiver operator characteristic curve).

Shuningdek, aniqlashning aniqligi (*precision*) va to‘liqligi (*recall*) baholash xarakteristikalari hisoblanadi. Anomal so‘rovni aniqlash tizimining aniqligi tajriba davomida qayta ishlangan misollarning qancha qismi haqiqatan ham anomal bo‘lib chiqqanligini ko‘rsatadi. To‘liqlik haqiqatdan ham anomal so‘rovlarning qancha qismi to‘g‘ri tasniflanganligini ko‘rsatadi.

Raqamli to‘liqlik haqiqiy ijobiy signallar darajasiga to‘g‘ri keladi, aniqlik (P) esa formula yordamida aniqlanadi:

$$P = \frac{N_{TP}}{N_{TP} + N_{FP}}$$

Muayyan muammolarni hal qilish uchun oldindan ustuvor xususiyat

belgilanadi. Shunday qilib, agar tizim natijada faqat yuqori darajadagi “ishonchlilik” ogohlantirish signalini berishi talab etilsa, unda aniqlikni oshirish zarur. Agar hujumlarning o‘tkazib yuborishni eng kichik soniga erishish talab etilsa, to‘liqlik xususiyati ustuvor hisoblanadi.

Aniqlik va to‘liqlikni o‘zida mujassamlashtirgan F-o‘lchov xususiyati ham mavjud bo‘lib- (F_1 Score, F bilan belgilanadi), aniqlik va to‘liqlikni garmonik o‘rtachasini namoyish qiladi, quyidagi formula bilan aniqlanadi:

$$F = 2\frac{PR_{TP}}{P + R_{TP}}$$

Samaradorlik xususiyatlarini aniqlagandan so‘ng, ma’lumotlar to‘plamidan anomal so‘rovlarni aniqlash uchun tizimning ishlashini baholash jarayoni ko‘rib chiqiladi. Samaradorlikning birinchi empirik tahlili k-pog‘onali kross-validatsiya uslubi yordamida amalga oshiriladi. Ushbu uslub barcha mavjud ma’lumotlarni k qismga bo‘lishni talab qiladi, bu yerda $1,\ldots,k-1$ qismlari o‘qitish uchun va k qismi testlash uchun ishlatiladi. Jarayon k qismning har biri testlash tanlanmasi sifatida ishlatilishi uchun k marta takrorlanadi. k-pog‘onali kross-validatsiya jarayoni quyidagi jadvalda ko‘rsatilgan.

Tajriba natijalarining statistik ahamiyatiga erishish uchun tajribaga ta’sir qilishi mumkin bo‘lgan tasodifiy ta’sirlarni istisno qilish uchun har bir tajribani bir necha marta takrorlash talab qilinadi. Ushbu ishda har bir tajriba 100 marta o‘tkazildi va natijada o‘rtacha arifmetik qiymat olindi [14].

3.2-jadval

k-pog‘onali kross-validatsiyadan foydalangan holda testlash uchun ma’lumotlarni tashkil qilish

Tajriba raqami	Ma’lumotlar qiamlari				
	1	2	3	…	k
1					
2					
3					
…	…	…	…	…	…

k					

Ishlab chiqilgan sun‘iy immunitet tizimining samaradorligi yuqorida tavsiflangan yondashuv yordamida sinovdan o‘tkazildi, bu yerda 10 pog‘onali kross-validatsiya usuli qo‘llanildi. Sun’iy immun tizimining modeli barcha elementlarning klaster markazlarigacha bo‘lgan masofalarining o‘rtacha arifmetik qiymatiga teng affinlik qiymati bilan sinovdan o‘tkazildi. Samaradorlikni tahlil qilishning vazifasi mos modelni tanlash, shuningdek, har bir model qo‘yilgan masalani qanchalik darajada yaxshi hal qilishini baholashdan iborat. Shunday qilib, mashinali o‘qitish modellarining samaradorlik ko‘rsatkichlari quyidagilarni o‘z ichiga oladi:

1. C_0 – to‘g‘ri tasniflangan anomal bo‘lmagan so‘rovlar foizi;
2. C_1 – to‘g‘ri tasniflangan anomal bo‘lgan so‘rovlar foizi;
3. R_{TP} – anomal deb tan olingan so‘rovlar haqiqatan ham qanchasi anomal bo‘lib chiqqanligini ko‘rsatuvchi haqiqiy ijobiy signallar darajasi;
4. R_{FP} – anomal bo‘lmagan so‘rovlarning qanchasi anomal bo‘lib chiqqanligini ko‘rsatuvchi yolg‘on ishga tushishlar darajasi;
5. P – tizimni ma’lum bir signalni berishda qanchalik “ishonchli”ligini tavsiflovchi aniqlik.
6. F – F-o‘lchov, aniqlik va to‘liqlik nuqtai nazaridan tasniflagichning umumiy ballini berish.

Aniqlik uchun eksperiment natijalarining o‘rtacha ko‘rsatkichlar modeli - haqiqiy ijobiy signallar darajalari (eng yuqori TP darajasiga ega konfiguratsiya) va yolg‘on ishga tushishlar darajalari (eng past FP darajasiga ega konfiguratsiya)ning o‘rtacha qiymatlari.

Logistik regressiya algoritmiga asoslangan klassifikator yordamida tajribalar natijalari quyidagi jadvalda keltirilgan.

3.3-jadval

Logistik regressiya algoritmi asosidagi klassifikatorning natijalari

	C_0(%)	C_1(%)	R_{TP}(%)	R_{FP}(%)	P(%)	F(%)
NSL-KDD DataSet	86	78	86	15	88	84
	83	75	84	17	87	83
CSIC 2010	86	92	92	14	89	91
	82	90	89	18	86	90
Enron Dataset	85	85	90	15	87	89
	83	83	88	17	85	87

Sun’iy neyron tarmog‘iga asoslangan klassifikator uchun 100 ta yashirin qatlamli neyronli ikki qatlamli perseptron modeli ishlatilgan.

3.4-jadval

Sun’iy neyron tarmoq asosidagi klassifikatorning natijalari

	C_0(%)	C_1(%)	R_{TP}(%)	R_{FP}(%)	P(%)	F(%)
NSL-KDD DataSet	87	89	87	13	88	90
	84	87	86	16	84	87
CSIC 2010	86	96	92	14	88	91
	82	95	89	18	86	90
Enron Dataset	85	95	90	15	88	90
	82	92	87	18	85	89

Muvofiqlikni tahlil qilish mexanizmidan foydalangan holda tavsiya etilgan sun’iy immun tizimiga asoslangan klassifikator. Yuqorida algoritmni ishlashini boshlash uchun ishga tushirish qiymatlari sifatida o‘rnatilishi kerak bo‘lgan bir nechta konstantalar keltirilgan. Ushbu konstantalarga quyidagilar kiradi:

- CL – klonlash darajasi;

- ML - mutatsiya darajasi.

Boshlash qiymatlari diapazonlari quyidagi jadvalda ko‘rsatilgan:

3.5-jadval

SIT ni ishga tushirish qiymatlari oralig‘i (N - natural, R – ratsional)

Parametr	**Qiymat oralig‘i**	**Tur**	**Tavsifi**
CL	≥1	*N*	Agar qiymat 1 ga teng bo‘lsa, xabar

			klonlanmaydi,
ML	[0,1]	R	Mutatsiyaga uchragan anomal so‘rovdagi atributlar ulushi (foizdagi nisbati)

Quyidagi jadvalda affinlik chegarasi bilan hisoblangan klassifikatorning samaradorlik ko‘rsatkichlari keltirilgan. Shuningdek, har bir tajriba uchun β - elementlar sonining β^m-elementlarga nisbati ko‘rsatilgan.

3.6-jadval

Sun’iy immun tizimiga asoslangan klassifikatorning natijalari

	Aff.	β^m/β **(%)**	C_0**(%)**	C_1**(%)**	R_{TP}**(%)**	R_{FP}**(%)**	***P*(%)**	***F*(%)**
NSL-KDD DataSet	0.01	22	98	96	96	2	97	96
		22	97	94	94	3	96	94
	0.05	19	96	94	93	4	95	94
		18	94	92	91	6	93	92
	0.1	16	95	91	90	5	93	92
		15	93	90	88	7	92	91
CSIC2010	0.01	22	96	95	96	4	96	95
		21	95	94	95	5	95	94
	0.05	21	95	93	94	5	94	93
		21	94	92	92	6	93	92
	0.1	21	94	91	92	6	92	91
		20	93	90	92	7	91	90
Enron Dataset	0.01	19	96	96	96	4	97	97
		19	95	95	95	5	96	95
	0.05	18	94	94	94	6	95	95
		17	95	93	93	5	94	95
	0.1	17	92	93	92	8	94	94
		16	92	9	91	8	93	93

3.3 Sun’iy immun tizimiga asoslangan anomaliyalarni aniqlash tizimini loyihalash

Tizimni amalga oshirish doirasida tuzilma sifatida uchta asosiy elementga (uch daraja) ega bo‘lgan hujumni aniqlash tizimi joriy qilingan korporativ tizim tanlandi:

1. Suqilib kirishlarni aniqlash tizimining ishlashi uchun zarur bo‘lgan ma’lumotlarni saqlovchi barcha ma’lumotlar bazasi tuzilmalarini amalga

oshiradigan ma’lumotlar bazasi serveri (server qismi). Amalga oshirish: MySQL, Oracle, Postgre, SQLite, MariaDB ma’lumotlar bazasi serverlari (tizimni amaliy tatbiq etish ushbu ma’lumotlar bazasi asosida amalga oshiriladi).

2. Ilova serveri, uning asosida ko‘p sathli suqilib kirishlarni aniqlash tizimi ishlaydi (server qismi). Amalga oshirish: dasturlash tillarida (C++, ASM, JAVA, PHP) amalga oshirilgan alohida dastur yoki xizmat.

3. Suqilib kirishlarni aniqlash tizimi bilan operator va tashqi tizimlar o‘rtasidagi o‘zaro aloqa uchun interfeyslarni amalga oshiruvchi taqdimot serveri (mijoz qismi). Amalga oshirish: taqdimot serverini amalga oshirish sifatida veb-server yechimi (Apache + NGINX) va asosiy ishlov berish tili sifatida (PHP) tanlandi [15].

Suqilib kirishlarni aniqlash tizimini mijoz-server ilovasining uch sathli arxitekturasi.

Taqdim etilgan suqilib kirishlarni aniqlash tizimini mijoz-server ilovasi ishlashi davomida ma’lumotlarni uzatishning quyidagi ketma-ketligini amalga oshiradi:

IDS Serveri -> Apache Serveri (veb-server yechimi) -> Ma’lumotlar bazasi Provayderi (*MariaDB*) -> Ma’lumotlar bazasi serveri (*MariaDB*) -> Ma’lumotlar bazasi provayderi (*MariaDB*) -> Interpretator (*PHP*) -> Veb-server (*Apache + NGINX*).

Axborotni uzatish ketma-ketligi quyidagi qadamlarni o‘z ichiga oladi:

- IDSda veb-server loglarini ishlov beruvchisi orqali Internet tarmog‘idan so‘rovlar kelib tushadi. So‘rovlar, dasturiy ta’minot yordamida, CSIC 2011 va Enron Dataset ma’lumotlar to‘plamida mavjud bo‘lgan so‘rovlar ko‘rinishiga keltiriladi;

- IDS adaptiv algoritmlaridan foydalanib ma’lumotlar bazasi provayderi (*MariaDB*) bilan o‘zaro aloqada bo‘lgan holda ushbu so‘rovlarni tahlil qiladi;

- ma’lumotlar bazasi provayderi (*MariaDB*) ma’lumotlar bazasidan (*MariaDB*) kerakli ma’lumotlarni yuboradi va qabul qiladi;

- mijoz (operator yoki boshqa tizim) ma’lumotlar bazasi provayderi (*MariaDB*) yordamida ma’lumotlar bazasiga so‘rovni vizual ko‘rsatish komponenti (mijoz-server ilovasining mijoz qismi) yoki API yordamida shakllantiradi;

- interpretator (PHP) va veb-server yordamida kerakli ma’lumotlar mijoz tomonidan (operator yoki boshqa tizimi) taqdim etiladi (namoyish qilinadi) .

Taklif qilingan mijoz-server ilovasi quyidagi ustunliklarga ega:

1. Xizmat ko‘rsatish (qo‘llab quvvatlash). Mijoz-server ilovasi lokal tarmoq tarkibidagi bir nechta mustaqil AT elementlari o‘rtasidagi axborot oqimini tahlil qilish vazifalarini taqsimlash funktsiyasini o‘z ichiga oladi.

2. Klasterli himoya. Suqilib kirishlarni aniqlash tizimlari tahlil qiladigan tugunlarga qaraganda yaxshi himoyalangan. IDS boshqariladigan serverga kirish nuqtasi bitta bo‘lib, operator yoki boshqa tizim tomonidan foydalaniladi.

3. Mijozlarning (terminallarning) samaradorlik va texnik xususiyatlariga nisbatan bo‘lgan past talablar natijasida ularning narxining pasayishi. Terminal sifatida nafaqat kompyuter, balki, smartfon yoki mobil telefon ham bo‘lishi mumkin.

4. Barcha suqilib kirishlarni aniqlash tizimlari uchun yagona mijoz [16].

Zaiflik tomonlari sifatida quyidagilarni keltirish mumkin:

1. Amalga oshirishning murakkabligi. Har bir tugun yoki ma’lumotlarni uzatish protokoli uchun alohida provayder yozish talab qilinadi.

2. Suqilib kirishlarni aniqlash tizimining boshqaruv tugunining ishlamasligi butun AT xavfsizlik tizimini ishlamay qolishiga olib keladi.

Testlarni o‘tkazish uchun tashkilotning ikkita tuguni (pochta serveri va veb-server) tanlab olindi, ularda mos ravishda IDS1 va IDS2 o‘rnatildi.

3.7-jadval

CSIC 2010 dagi so‘rovlar formati bo‘yicha to‘plamlar

№	To‘plam nomi	Yozuvlar soni	Tavsifi
1	*Anomalous test*	4786	Anomal so‘rovlar to‘plamlari
2	*Normal training*	15618	Test so‘rovlar to‘plamlari
3	*“Full” dataset*	59843	Anomal va test so‘rovlar to‘plamlari (oddiy trafik)

3.8-jadval

Enron Dataset dagi so‘rovlar formati bo‘yicha to‘plamlar

№	To‘plam nomi	Yozuvlar soni	Tavsifi
1	*Spam*	1755	Anomal so‘rovlar to‘plamlari
2	*Ham*	2375	Test so‘rovlar to‘plamlari
3	*Raw dataset*	12539	Anomal va test so‘rovlar to‘plamlari (oddiy trafik)

3.9-jadval

Sun’iy immun tizimiga asoslangan klassifikatorning natijalari

	Aff.	β^m/β **(%)**	C_0**(%)**	C_1**(%)**	R_{TP}**(%)**	R_{FP}**(%)**	***P*(%)**	***F*(%)**
IDS1	0.01	22	97	96	96	3	92	95
		22	96	94	94	4	91	93
	0.05	19	95	94	93	5	90	93
		18	95	92	91	5	88	91
	0.1	16	94	91	90	6	88	91
		15	94	90	88	6	87	90
IDS2	0.01	21	94	93	94	6	92	93
		20	94	92	93	6	91	92
	0.05	20	93	91	92	7	90	91
		20	92	90	90	8	89	90
	0.1	19	92	89	90	8	89	89
		18	91	88	89	9	87	88

Shunday qilib, olingan natijalar yuqorida olingan natijalar bilan to‘liq mos keladi. Bundan kelib chiqqan holda, taklif etilayotgan adaptiv algoritmlar bo‘yicha ishlaydigan suqilib kirishlarni aniqlash tizimlari, shu jumladan sun’iy immun tizimi korxona lokal tarmoq tarkibida qo‘llanilishi mumkinligini ta’kidlash mumkin.

3-bob bo‘yicha xulosa

Magistrlik dissertatsiya ishining uchinchi bobida su’niy immun tizimiga asoslangan anomal so‘rovlarni aniqlashning tizimini loyihalash amalga oshirildi, quyidagi natijalar olindi:

- su’niy immun tizimiga asoslangan suqilib kirishlarni aniqlash tizimining arxitekturasi tegishli mantiqiy elementlar va ularning ishlash bosqichlaridan hamda anomaliyalarni aniqlash algoritmi tadqiq etildi;

- suqilib kirishlarni aniqlashda mashinali o‘qitishga asoslangan anomaliyalarni aniqlash mexanizmi ishlash jarayoni samaradorligini tahlil qilindi;

- mijoz-server arxitekturasiga asoslangan sun’iy immun tizimiga asoslangan anomaliyalarni aniqlash tizimini loyihalash amalga oshirildi;

XULOSA

Magistrlik dissertatsiya ishida axborot tizimlari anomaliyalarini sun’iy immun tizimlar asosida aniqlash mexanizm va algoritmlari tadqiq qilinib, quyidagi natijalar olindi:

- axborot tizimida saqlanadigan va ma’lumotlarni uzatish jarayonida axborotni xavfsizligiga nisbatan tarmoqdan bo‘ladigan tahdidlar tavsifi va tasnifi ko‘rib chiqildi;
- tajavuzkor tomonidan tashkilotning tarmog‘iga tashqaridan bo‘ladigan hujumlarni amalga oshirish bosqichlari hamda tasnifi ko‘rib chiqildi, mavjud zaifliklar va kamchiliklardan foydalanib himoyalash tizimining foydalanuvchanligini buzilishiga qaratilgan suqilib kirishlarni aniqlash va bartaraf etish tizimlarida qo‘llaniladigan yondashuvlar tadqiq va tahlil qilindi;
- mashinali o‘qitish tizimlarini o‘qitish va sinovdan o‘tkazishda qo‘llaniladigan ma’lumotlar to‘plamlari NSL-KDD ISCX Dataset, CSIC 2010 Dataset, Enron Dataset tadqiq va tahlil qilindi;
- - tarmoqni himoyalashda suqulib kirishlarni aniqlash tizimlarini loyihalashda qo‘llaniladigan sun’iy immun tizimi tuzilmasi va unga qo‘yiladigan talablar ko‘rib chiqildi hamda loyihalashda qo‘llaniladigan elementlari tadqiq qilindi;
- su’niy immun tizimiga asoslangan suqilib kirishlarni aniqlash tizimining arxitekturasi tegishli mantiqiy elementlar va ularning ishlash bosqichlaridan hamda anomaliyalarni aniqlash algoritmi tadqiq etildi;
- suqilib kirishlarni aniqlashda mashinali o‘qitishga asoslangan anomaliyalarni aniqlash mexanizmi ishlash jarayoni samaradorligi tahlil qilindi va mijoz-server arxitekturasiga asoslangan sun’iy immun tizimiga asoslangan anomaliyalarni aniqlash tizimini loyihalash amalga oshirildi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasi Prezidentining Farmoni, 2022 — 2026-yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida. 2022-yil.
2. O‘zbekiston Respublikasining Qonuni, Kiberxavfsizlik to‘g‘risida. 2022-yil.
3. S.K. Ganiev, A.A. Ganiyev, Z.T. Xudoyqulov, “Kiberxavfszilik asoslari”, Iqtisod-Moliya, Toshkent, 2021.
4. L. Nunes, J. Timmis, Artificial Immune Systems: A New Computational Intelligence Approach – Springer Science & Business Media, 2012. – P. 2-10.
5. S. Abe, Support Vector Machines for Pattern Classification – Springer Science & Business Media, 2015. – P. 39-41.
6. S. Kollias, Artificial Neural Networks – Springer Science & Business Media, 2016. – 161 p.
7. P. Bentley, D. Lee, S. Jung, Artificial Immune Systems – 7th International Conference ICARIS-2015, 2015. – P. 200-202.
8. R. Pietro, Intrusion Detection Systems – Springer Science + Business Media LTD, 2015. – 210 p.
9. M. Tavallaee, E. Bagheri, W. Lu, A. Ghorbani, A Detailed Analysis of the KDD CUP 99 Data Set – Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2015.
10. R.S. Rajesh, K.S. Easwarakumar, R. Balasubramanian., Computer Networks: Fundamentals & Applications – New Delhi: Vicas Pub, 2016. – P. 19-25.
11. I. Mann, Hacking the Human: Social Engineering Techniques and Security Countermeasures – Gover Publishing Ltd, 2016. – 273 p.
12. D.K. Bhattacharyya, Network Anomaly Detection: A Machine Learning Perspective– CRC Press, 2013. – 191 p.

13. М.Е. Бурлаков, Двухклассификационная искусственная иммунная система – Самара: Вестник Самарского государственного университета, 2014. – №7(118). – С. 207-221.

14. М.Е. Бурлаков, Исследование динамики активности публикации угроз в открытых и закрытых источниках – Самара, Перспективные информационные технологии (ПИТ-2017): труды Международной научно-технической конференции. – 2017 – С. 315-320.

15. Burlakov, Research the dynamic of author activities in threats through to public and private sources – Samara: Information Technology and Nanotechnology – 2017 Information Security, 2017 – P. 958-961.

16. . Kotov V.D., V.I. Vasilyev Artificial Immune Systems Based Intrusion Detection System. – Proceedings of the Second Intrnational Conference on Security of Information and Networks (SIN’09), 2009 – P. 207-212.

17. Protic D.D. 2020. Influence of preprocessing on anomaly-based intrusion detection. Vojnotehnički glasnik/Military Technical Courier, 68(3), pp.598-611.

18. Sri Lakshmi, K. 2014. Implementation of Artificial Immune System Algorithms. International Journal of Application or Innovation in Engineering and Management (IJAIEM), 3(6), pp.367-372.

19. Tavallaee, M., Bagheri, E., Lu, W. & Ghorbani, A.A. 2009. A detailed analysis of the KDD CUP 99 data set. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, July 8-10.

20. Xishuang, D., Multi-word-Agent Autonomy Learning Based on Adaptive Immune Theories, JDCTA Int. J. Digit. Content Technol. its Appl., vol. 7, no. 3, pp. 723–745, 2013.

21. Hosseinpour F., Meulenberg A., Ramadass S., Vahdani Amoli P., and Z. Moghaddasi, Distributed Agent Based Model for Intrusion Detection System Based on Artificial Immune System, Int. J. Digit. Content Technol. its Appl., vol. 7, pp. 206–214, 2013.