TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

G'ULOMOV SHERZOD RAJABOYEVICH

AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA TARMOQ TRAFIGINI FILTRLASHNING USULI VA VOSITALARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI DOKTORI (DSc) DISSERTATSIYASI AVTOREFERATI

Toshkent-2024

UDK: 004.056.57

Texnika fanlari doktori (DSc) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора (DSc) по техническим наукам

Contents of dissertation abstract of the doctor (DSc) on technical sciences

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

G'ULOMOV SHERZOD RAJABOYEVICH

AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA TARMOQ TRAFIGINI FILTRLASHNING USULI VA VOSITALARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI DOKTORI (DSc) DISSERTATSIYASI AVTOREFERATI

Toshkent-2024

Texnika fanlari doktori (DSc) dissertatsiyasi mavzusi O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2024.1.DSc/T770 raqam bilan ro'yxatga olingan.

Dissertatsiya Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o'zbek, rus, ingliz (rezyume)) Ilmiy kengash veb-sahifasida (www.tuit.uz) va "Ziyonet" Axborot ta'lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy maslahatchi:	**Karimov Madjit Malikovich** texnika fanlari doktori, professor
Rasmiy opponentlar:	**Raxmatullayev Marat Alimovich** texnika fanlari doktori, professor
	Kerimov Kamil Fikratovich texnika fanlari doktori, dotsent
	Kuryazov Davlatyor Matyakubovich fizika-matematika fanlari doktori
Yetakchi tashkilot:	**Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.02 raqamli Ilmiy kengashning 2024-yil 29-iyun soat 11:00 dagi majlisida bo'lib o'tadi. (Manzil: 100084, Toshkent shahri, Amir Temur ko'chasi, 108-uy. Tel.: (99871) 238-64-43, faks: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Dissertatsiya bilan Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot-resurs markazida tanishish mumkin (№ 317 raqam bilan ro'yxatga olingan). (Manzil: 100084, Toshkent shahri, Amir Temur ko'chasi, 108-uy. Tel.: (99871) 238-65-44).

Dissertatsiya avtoreferati 2024-yil 21-iyunda tarqatildi.
(2024-yil 21-iyundagi № 13 raqamli reyestr bayonnomasi.)

B.Sh. Maxkamov
Ilmiy darajalar beruvchi Ilmiy kengash raisi, iqtisodiyot fanlari doktori, professor

M.S. Saitkamolov
Ilmiy darajalar beruvchi Ilmiy kengash ilmiy kotibi, iqtisodiyot fanlari doktori, dotsent

S.K. Ganiyev
Ilmiy darajalar beruvchi Ilmiy kengash qoshidagi Ilmiy seminar raisi, texnika fanlari doktori professor

KIRISH (fan doktori (DSc) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Butun dunyo bo'ylab axborot-kommunikatsiya tizimlarining tez sur'atlarda rivojlanishi va joriy etilishi natijasida foydalanuvchilarga taqdim etilgan imkoniyatlar bilan bir qatorda tarmoqlarda tahdid va hujumlarning ulushi ham ortib bormoqda. Dunyodagi AyTi kompaniyalarining statik ma'mulotlari tahlili natijasidan xulosa qilish mumkinki, axborot-kommunikatsiya tizimlarida DDoS hujumlarining amalga oshirilishi darajasi yuqori. Xususan, CloudFlare kompaniyasi ma'lumotlariga ko'ra 2023-yilning ikkinchi choragida HTTP DDoS hujumlari hajmi birinchi chorakdagiga nisbatan 15% ga, uchinchi chorakda esa bu ko'rsatgich 65% ga oshganligini[1] ko'rish mumkin. Alohida ta'kidlash kerakki, deyarli barcha turdagi hujumlarni amalga oshishiga hujumlarni aniqlash tizimlari va tarmoqlararo ekranlarning sozlashdagi kamchiliklar va hujumlarni bartaraf etishning yetarlicha modullarga ega emasliklari sabab bo'lgan. Tarmoq paketlari qoidalarini optimallashtirish, tarmoq trafigidagi anomal holatlarni aniqlash va identifikatsiyalashning axborot modellarini takomillashtirish, tarmoqda bo'ladigan hujumlarni aniqlash va bartaraf etish, tarmoq trafigini filtrlash usullari va algoritmlarini ishlab chiqish AQSh, Xitoy Xalq Respublikasi, Rossiya Federatsiyasi, Buyuk Britaniya, Irlandiya, Germaniya, Italiya, Ispaniya, Braziliya, Yaponiya, Janubiy Koreya va boshqa davlatlarda muhim ahamiyat kasb etmoqda.

Jahon tajribasiga ko'ra, axborot-kommunikatsiya tizimlarida tarmoq hujumlarini aniqlash va bartaraf etishga asoslangan trafikni filtrlash modellarini, usullarini va algoritmalarini, tarmoq paketlaridagi anomaliyalarni aniqlash usullarini va shubhali paketlarni aniqlash vositalarini ishlab chiqishga qaratilgan ilmiy-amaliy tadqiqot ishlari olib borilmoqda. Axborot-kommunikatsiya tizimlarida tarmoq trafigini filtrlashning usul va vositalarini ishlab chiqish bo'yicha olib borilgan izlanishlar natijasida bir qator ilmiy natijalarga erishildi, jumladan, ma'lumotlar proksi-serverlari va kognitiv tarmoqlararo ekranlar ishlab chiqilgan (Massachusets texnologiyalar instituti, AQSh); uzatish blokini o'zgartirish funksiyasi va atribut qiymatini xaritalash funksiyasini qo'shish orqali COAST tarmoqlararo ekran mos yozuvlar modelining imkoniyatlari takomillashtirilgan (Zhejiang universiteti, Xitoy Xalq Respublikasi); protokollar va xizmatlarni tasniflash, OSI modelining tarmoq sathidan ilova sathigacha turli darajadagi trafikni kuzatish va blokirovka qilishga imkon beruvchi Next Generation Firewall yangi avlod tarmoqlararo ekrani ishlab chiqilgan (TexArgos kompaniyasi, Rossiya Federatsiyasi); tarmoq xavfsizligini samarali ishlashga xizmat qiluvchi ruxsat berish va rad etish algoritmlari ishlab chiqilgan va mininet nomli tarmoq simulyatsiya platformasi asosida algoritmning samaradorligi isbotlangan (Jon Hopkins universiteti, AQSh); paketlarni filtrlash qoidalarini optimallashtirish asosida fishing hujumlari sonini kamaytiruvchi himoya strategiyasi va Honeypot tizimi ishlab chiqilgan (Aydaho Davlat universiteti, AQSh); tarmoqlararo ekranlarni Networks-on-Chip (NoC) marshrutizatorlari orasiga o'rnatish orqali paket sarlavhalarida ma'lumotlar xavfsizligini ta'minlovchi

[1] https://blog.cloudflare.com/ddos-threat-report-2023-q3/

usul ishlab chiqilgan (Myunxen texnika universiteti, Germaniya va San-Paulu universiteti, Braziliya). Bu borada, paketlarni filtrlash qoidalarini optimallashtirish, SDN tarmoqlarida trafikni filtrlashni amalga oshirish usullari, ishchi stansiyalarda zararli tarafikni aniqlash algoritmlari va veb-resurslarni filtrlash arxitekturalarini takomillashtirish va ishlab chiqish hozirgi kunning dolzarb muammolaridan biri hisoblanmoqda. Ushbu muammolarni yechish maqsadida bir qator yangi turdagi hujumlarni aniqlash, baholash va ularni bartaraf etish usullari va vositalarini takomillashtirishni ilmiy tomondan asoslash talab etiladi.

Respublikamiz miqyosida davlat va xo'jalik boshqaruv hamda mahalliy davlat hokimiyati organlarida tarmoqni ichki va tashqi hujumlardan himoyalash jarayonida tarmoq trafigini filtrlashning usul va vositalarini takomillashtirishga qaratilgan keng qamrovli ishlar amalga oshirilmoqda. 2022-2026-yillarga mo'ljallangan Yangi O'zbekistonning Taraqqiyot strategiyasi to'g'risidagi «..."UZ" domen zonasi Internet-makonining kiberxavfsizligini ta'minlashning asosiy yo'nalishlarini hamda elektron hukumat, energetika, raqamli iqtisodiyot tizimlarini va muhim axborot infratuzilmasiga taalluqli boshqa yo'nalishlarni himoya qilish bo'yicha kompleks vazifalarni belgilash...»[2] vazifalari keltirilgan. Mazkur vazifalarni bajarishda, axborot-kommunikatsiya tizimlarida tarmoq paketlari anomaliyalarini aniqlash modellarini, tarmoq paketlarini filtrlash usullari va algoritmlarini hamda tarmoqda shubhali paketlarni bartaraf etish vositalarini takomillashtirish va ishlab chiqish muhim hisoblanadi.

O'zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son "2022 – 2026-yillarga mo'ljallangan Yangi O'zbekistonning Taraqqiyot strategiyasi to'g'risida" gi Farmoni, 2022-yil 22-avgustdagi PQ-357-son "2022-2023-yillarda axborot-kommunikatsiya texnologiyalari sohasini yangi bosqichga olib chiqish chora-tadbirlari to'g'risida"gi, 2019-yil 14-sentabrdagi PQ-4452-son "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi Qarorlari, 2018-yil 19-fevraldagi PF-5349-son "Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to'g'risida"gi Farmoni va 2018-yil 21-noyabrdagi PQ-4024-son "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to'g'risida"gi Qarori hamda mazkur faoliyatga mansub boshqa me'yoriy va normativ-huquqiy hujjatlar asosida belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya ishi ma'lum darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo'nalishlariga mosligi. Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining IV. «Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish» ustuvor yo'nalishi doirasida bajarilgan.

Dissertatsiya mavzusi bo'yicha ilmiy-tadqiqotlar sharhi[3]. Axborot-

[2] O'zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi PF-60-son «2022 - 2026 yillarga mo'ljallangan Yangi O'zbekistonning Taraqqiyot strategiyasi to'g'risida» gi Farmoni

[3] Dissertatsiya mavzusi bo'yicha ilmiy tadqiqotlar sharhi https://link.springer.com, https://www.researchgate.net, www.elsevier.com, https://scholar.google.com, https://habr.com va boshqa manbalar asosida shakllantirilgan.

kommunikatsiya tizimlarida tarmoq trafigini filtrlashning usul va vositalarini ishlab chiqishga qaratilgan ilmiy tadqiqotlar dunyoning eng ilg'or va yetakchi ilmiy tekshirish institutlari, ilmiy-tadqiqot markazlari va oliy o'quv yurtlarida, shu jumladan Sababa Security kompaniyasi (Italiya), Cybergamp kompaniyasi (Ispaniya), Geedge Networks (Xitoy Xalq Respublikasi), Oksford universiteti (Buyuk Britaniya), London Imperial kolleji (Buyuk Britaniya), Massachusets texnologiya instituti (AQSh), Berkeley, Kaliforniya universiteti (AQSh), Jon Hopkins universiteti (AQSh), Shimoliy Djorjiya universiteti (AQSh), Aydaho Davlat universiteti (AQSh), Dublin Siti universiteti (Irlandiya), Myunxen texnika universiteti (Germaniya), Zhejiang universiteti (Xitoy Xalq Respublikasi), N.E.Bauman nomidagi Moskva davlat texnika universiteti (Rossiya Federatsiyasi), TexArgos kompaniyasi (Rossiya Federatsiyasi), Janubiy Koreya fan va texnologiya ilmiy instituti (Janubiy Koreya), Tokio texnologiya instituti (Yaponiya), Waseda universiteti (Yaponiya), San-Paulu universiteti (Braziliya) va respublikamizda Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti, Toshkent shahridagi Inxa universiteti, Raqamli texnologiyalar va sun'iy intellektni rivojlantirish ilmiy-tadqiqot instituti, "Kiberxavfsizlik markazi" davlat unitar korxonasi, "UNICON.UZ" Fan-texnika va marketing tadqiqotlari markazi davlat unitar korxonasida olib borilmoqda.

Muammoning o'rganilganlik darajasi. Denis Salopek real vaqtda paketlarni filtrlash uchun gibrid apparat/dasturiy vositalarni ishlab chiqish, Chun-Liang Lee, Guan-Yu Lin, Yaw-Chung Chen kabi tadqiqotchilar ko'p o'lchovli paketlarni filtrlashda ziddiyatni tezkor aniqlash algoritmlarini ishlab chiqish bo'yicha ilmiy izlanishlar olib borganlar. Luis A.Trejo, Viktor Ferman, Miguel Angel Medina-Perez, Fernando Miguel Arredondo Giacinti, Raul Monroy, Jose Emanuel Ramirez-Marquez kabi tadqiqotchilar DNS-ADVP: Mashinali o'qitish orqali anomaliyalarni aniqlash va yuqori darajadagi domen nomlari serverlarini DDoS hujumlaridan himoya qilish uchun vizual platformalarni tatbiq qilish bo'yicha ilmiy tadqiqotlar olib borgan. Joker belgilarsiz bir nechta maydonlar asosida SDN paketlarini segmentlashning umumiy yondashuvlari bo'yicha H.Alimohammadi, M.Ahmadi kabi olimlar tomonidan ilmiy izlanishlar olib borilgan va hozirda ham ular boshchiligidagi ilmiy maktablar tomonidan davom ettirilmoqda. Bundan tashqari, Palo Alto Networks, InfoWatch, McAfee, Fortinet, Crowdstrike, Trend Micro, SababaSecurity, CyberGamp, Gen Digital, IBM, CyberArk va Cisco kompaniyalari va tashkilotlari tomonidan tarmoq paketlari qoidalarini optimallashtirish va yangi turdagi apparat-dasturiy tarmoqlararo ekranlarni ishlab chiqishga qaratilgan ilmiy-amaliy va muhandislik-tadqiqot ishlari olib borilmoqda.

O'zbekistonda T.F.Bekmuratov, S.K.G'aniyev, M.M.Karimov, R.H.Hamdamov, A.A.Ganiyev, K.A.Tashev, Z.T.Xudoykulov, N.B.Nasrullayev, O.M.Allanovlar rahbarligidagi ilmiy jamoalar tomonidan axborot-kommunikatsiya tizimlarida suqilib kirishlarni aniqlash va bartaraf etish, axborot xavfsizligini ta'minlash modellarini boshqarish, kompyuter tarmoqlarida foydalanishni cheklashning usul va vositalari samaradorligini oshirish bo'yicha ilmiy izlanishlar

olib borilmoqda.

Shu bilan birga, axborot-kommunikatsiya tizimlarida tarmoq trafigida anomaliyalar va noqonuniy harakatlarni aniqlash tizimlari, DNS serverlarida zararli trafikni bartaraf etish modeli, tarmoq hujumlarini bartaraf etishda DSCPga asoslangan trafikni filtrlash va SDN tarmoqlarida trafikni filtrlashni amalga oshirish usullari hamda trafikni filtrlash qoidalarini optimallashtirish algoritmlari yetarlicha tadqiq etilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta'lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog'liqligi. Dissertatsiya tadqiqoti Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining ilmiy-tadqiqot ishlari rejasining 598661-EPP-12018-1-RO-EPPKA2-CBHE-JP "Developing Services for Individuals with Disabilities–DECIDE" (2019-2022), 598092-EPP-1-2018-1-BG-EPPKA2-CBHE-SP "Modernization of Higher Education in Central Asia through New – HiEdTec" (2019-2022) va «UNICEN loyihasi "Accreditation, Assessment and Improving Student Outcomes" (2021-2022) mavzusidagi loyihalar doirasida bajarilgan.

Tadqiqotning maqsadi axborot-kommunikatsiya tizimlarini himoyalash samaradorligini oshirishga imkon beruvchi tarmoq trafigini filtrlashning usul va vositalarini takomillashtirish va ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

axborot-kommunikatsiya tizimlarida tarmoq trafigining o'tkazuvchanlik qobiliyatini o'lchash usullarini tasniflash va tarmoq trafigini filtrlash usullarini qiyosiy tahlillash;

tarmoq trafigida anomal holatlarni aniqlash va identifikatsiyalashning axborot modelini ishlab chiqish;

DNS serverlarida bo'ladigan zararli trafikni bartaraf etish va u bilan bog'liq hujumlardan himoyalanish modelini takomillashtirish;

differensial xizmatlarning kod nuqtasi asosida tarmoq trafigini filtrlash usulini takomillashtirish;

tarmoq paketlarining yo'qolishini minimallashtirish va ularning xizmat ko'rsatish sifatini oshirish usulini takomillashtirish;

tarmoq trafigi xatti-harakatlariga muvofiq paketlarni filtrlash qoidalarida risklarni aniqlash algoritmlarini ishlab chiqish;

tarmoq trafigida veb-resurslarni zararli botlar va shubhali paketlardan himoyalash algoritmlarini ishlab chiqish.

Tadqiqotning obyekti sifatida tarmoq xavfsizligi kontekstida axborot-kommunikatsiya tizimlarining ma'lumotlar oqimi olingan.

Tadqiqotning predmetini axborot-kommunikatsiya tizimlarida tarmoq trafigini filtrlash tashkil etadi.

Tadqiqotning usullari. Tadqiqotda ehtimollar nazariyasining asosiy tamoyillari, axborotni himoyalash usullari, matematik modellashtirish, sun'iy intellekt, obyektga yo'naltirilgan dasturlash tillari, shuningdek, dasturiy vosita yordamida ularning ishonchliligini aniqlash uchun tajribaviy tadqiqotlar natijalariga asoslangan usullardan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

tarmoq trafigi faoliyatini baholash va monitoringlash asosida tarmoqda yuzaga keluvchi zaifliklar va nosozliklar holatlari haqida ogohlantirishlar berish orqali tashqi tahdidlar ta'sirini minimallashtirish hamda tarmoq anomaliyalarini identifikatsiyalashning axborot modeli ishlab chiqilgan;

mashinali o'qitish usullari asosida DNS serverlariga bo'ladigan zararli so'rovlarni aniqlash va blokirovka qilish hamda DNS-trafik bilan bog'liq boshqa turdagi, jumladan, DDoS hujumlaridan himoyalashning zararli trafikni bartaraf etish modeli takomillashtirilgan;

differensial xizmatlarning kod nuqtasi asosida tarmoqda IP-manzilli nizolar xavfini kamaytirish hamda DHCP paketlarining maksimal sonini cheklash qoidasini o'rnatish orqali DHCP serverining ortiqcha yuklanishini bartaraf etishning filtrlash usuli takomillashtirilgan;

TCP psevdo-sarlavhasini qo'shish orqali tarmoq trafigi oqimini normallashtirish, ma'lumotlar almashinuvini niqoblash va uzatiladigan tarmoq paketlari kechikishini boshqarish hamda sensorlar korrelyatsiyasi yordamida tarmoq trafigida xizmat sifatini oshirish va tarmoq paketlarining yo'qolishini minimallashtirish usuli takomillashtirilgan;

tarmoq trafigi xatti-harakatlariga muvofiq axborot xavfsizligi risklarini minimallashtirish va noravshan filtrlashni qo'llash orqali paketlarni filtrlash unumdorligini oshirish hamda tarmoq paketlarini qabul yoki rad etishda qoidalarning eng yuqori ustuvorligini aks ettirish algoritmlari ishlab chiqilgan;

veb-so'rovlarni ishlash bloklari asosida veb-resurslarni zararli botlardan himoya qilish, veb-sahifalarni haqiqiyligini tekshirish, domenlarni onlayn tahdidlar va soxta fishing hujumlaridan himoya qilish hamda tizimda bo'ladigan yolg'on xabarlarni minimallashtirish algoritmlari ishlab chiqilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

SDN tarmoqlarida orkestrator va paketlarni filtrlash modullari asosida trafik oqimlarini monitoringlash hamda tarmoqda suqilib kirishi mumkin bo'lgan har qanday zararli yoki istalmagan kontentni bartaraf etish usuli takomillashtirilgan;

tarmoq trafigida tarmoqlararo ekrandagi tugunlar soni ortishi bilan tarmoq paketlari qoidalarini ishlash vaqtini kamaytirish, paketlarning to'lib-toshishi va ortiqchaligi hamda tarmoqda bo'ladigan IP-Spoofing hujumlarini minimallashtirishga imkon beruvchi filtrlash algoritmlari optimallashtirilgan;

giperhavola funksiyalaridan foydalanish hisobida veb-sahifalarni haqiqiyligini tekshirish, domenlarni soxta fishing hujumlaridan hamda onlayn tahdidlar va nol hujumlaridan himoyalash algoritmi ishlab chiqilgan;

ko'p faktorli trafik tahlili asosida DDoS hujumlari so'rovlarini blokirovkalash, ochiq VPN xizmatini amalga oshirish, URL filtri jurnallarini nazoratlash, axborotni lokatsiya bo'yicha filtrlash, IP-tables ishlashini amalga oshirish va tizimga zararli kodlar kirishini minimallashtirish dasturiy vositasi ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi. Tadqiqotda qo'llanilgan yondashuv va usullarning maqsadga muvofiqligi, ma'lumotlarning rasmiy manbalardan, jumladan, "Kiberxavfsizlik markazi" DUK davlat unitar korxonasining statistik

ma'lumotlaridan olinganligi hamda tegishli xulosa va takliflarning mutasaddi tashkilotlar tomonidan amaliyotga joriy etilganligi bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati takomillashtirilgan axborot-kommunikatsiya tizimlarida anomal holatlarni aniqlash va identifikatsiyalashning axborot modeli, DNS serverlarida bo'ladigan zararli so'rovlarni aniqlash va bartaraf etish modeli, differensial xizmatlarning kod nuqtasi asosida tarmoq trafigini filtrlash usuli, tarmoq paketlarining yo'qolishini minimallashtirish va ularning xizmat ko'rsatish sifatini oshirish usuli, tarmoq paketlari qoidalari algoritmlarini takomillashtirish va optimallashtirish hamda tarmoq trafigida axborotni himoyalash tizimlarini rivojlantirishga xizmat qiladi.

Tadqiqot natijalarining amaliy ahamiyati taklif etilgan modellar, usullar va algoritmlar asosida ishlab chiqilgan dasturiy vosita yordamida tarmoq paketlarida mavjud risklarni minimallashtirish, veb-resurslarni zararli botlardan va shubhali trafikdan himoyalash, DDoS hujumlari so'rovlarini blokirovkalash, ochiq VPN xizmatlarini amalga oshirish, URL filtri jurnallarini nazoratlash, axborotni lokatsiya bo'yicha filtrlash hamda tizimga zararli kodlarning kirishini minimallashtirish bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Axborot-kommunikatsiya tizimlarida tarmoq trafigini filtrlashning usul va vositalari bo'yicha olingan ilmiy natijalar asosida:

veb-hujumlardan himoyalashda veb-resurslarni filtrlash arxitekturasi asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi Toshkent shahar Mirzo Ulug'bek tumani hokimligi axborot tizimining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2024-yil fevraldagi 33-8/916-son ma'lumotnomasi). Ilmiy tadqiqot natijasida UzFirewall-next generation firewall dasturiy vositasi Kerio Control 8.3.0 vositasi bilan solishtirganda ma'lumotlarni uzatish tezligi 1 Gbit/s va o'rtacha paket hajmi 12000 bit bo'lganda, 2,7 barobar tezroq ishlash imkonini bergan, ya'ni Kerio Control 8.3.0 vositasida paketlarni qayta ishlash vaqti 0,000005, UzFirewall-next generation firewall dasturiy vositasida esa 0,000002 soniyalarni tashkil qilgan;

IP-manzilli nizolar xavfini kamaytirish hamda DHCP paketlarining maksimal sonini cheklash qoidasini o'rnatish orqali DHCP serverining ortiqcha yuklanishini bartaraf etish usuli va giperhavola funksiyalaridan foydalanib veb-sahifaning qonuniyligini tekshirish hamda domenlarni soxta fishing hujumlardan hamda onlayn tahdidlar va nol hujumlardan himoya qilish algoritmlari asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi O'zbekiston Respublikasi madaniyat vazirligining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2024-yil fevraldagi 33-8/916-son ma'lumotnomasi). Tadqiqot natijasida UzFirewall-next generation firewall dasturiy vosita vazirlikning axborot tizimida mumkin bo'lgan tarmoq hujumlarini 96% aniqlik bilan aniqlash va bartaraf etishga imkon bergan;

trafik xatti-harakatlariga muvofiq qoidalar harakatlarini o'zgartirish, muhim ma'lumotlar uchun yuqori darajadagi xizmatni taqdim etish va tarmoq xizmati sifatini oshirish hamda tarmoq paketlarini qabul va bekor qilishda qoidalarning eng

yuqori ustuvorligini aks ettirish arxitekturasi va algortimlari asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi huzuridagi "O'zkomnazorat" inspeksiyasi Toshkent shahar hududiy bo'limi korporativ tarmog'ining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2024-yil fevraldagi 33-8/916-son ma'lumotnomasi). Ilmiy tadqiqot natijasida UzFirewall-next generation firewall dasturiy vositasi o'zining asl maksimal o'tkazuvchanlik holatidan 3 baravar unumdor ishlashga imkon bergan, bunda nisbiy masshtablilik qobiliyati 300% ni tashkil etgan hamda mazkur vositada normal yuklanish ishlashiga nisbatan maksimal yuklanish 250% ga, ya'ni 2,5 marta oshganligi aniqlangan;

TCP psevdo-sarlavha qo'shish orqali tarmoq trafigi oqimini optimallashtirish, tarmoqni ishdan chiqish holatlarini kamaytirish, TCP psevdo-sarlavha port raqamini o'zgartirish orqali ma'lumotlar almashinuvini niqoblash va uzatiladigan tarmoq paketlari kechikishini boshqarish usuli asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi O'zbektelekom AK "Samarqand shahar telekommunikatsiya bog'lamasi" aloqa va telefoniya tarmog'ining amaliy faoliyatiga joriy etilgan (Raqamli texnologiyalar vazirligining 2024-yil fevraldagi 33-8/916-son ma'lumotnomasi). Ilmiy tadqiqot natijasida UzFirewall-next generation firewall dasturiy vositasi tarmoq trafigida shubhali paketlarni blokirovkalashda 95% samarali ishlash imkonini bergan. Mazkur dasturiy vositadan foydalanish tashkilotning tarmoq tizimidagi ma'lumotlarini filtrlash va ulardagi shubhali paketlarni yuqori aniqlikda aniqlash imkoniga ega bo'lish bilan bir qatorda, tashkilotning axborot tarmog'idagi axborot xavfsizligini ta'minlash samaradorligini oshirishga ham imkon bergan;

SDN tarmoqlarida trafikni filtrlashni amalga oshirish usullari va ishchi stansiyalarda zararli tarafikni aniqlash algoritmlari asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Bilim va malakalarni baholash agentligi korporativ tarmog'ining amaliy faoliyatiga joriy etilgan (O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligining 2024-yil fevraldagi 3/22-21/02-02-son ma'lumotnomasi). Tadqiqot natijasida UzFirewall-next generation firewall dasturiy vositasining 2 soat mobaynida tarmoq hujumlariga o'rtacha javob vaqti 2,6 daqiqani tashkil etdi. Yuqorida keltirilgan natijalardan ko'rinib turibdiki, mazkur dasturiy vosita hujumlarga tezroq javob qaytarish imkonini bergan;

paketlarni filtrlash qoidalari algoritmlarini takomillashtirish va optimallashtirish natijasida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi "UZINFOCOM Davlat axborot tizimlarini yaratish va qo'llab-quvvatlash bo'yicha yagona integrator" MChJ korporativ tarmog'ining amaliy faoliyatiga joriy etilgan (Raqamli texnologiyalar vazirligining 2024-yil fevraldagi 33-8/916-son ma'lumotnomasi). Ilmiy tadqiqot natijasida UzFirewall-next generation firewall dasturiy vositasi 1 soat mobaynida tizimda 11230 paketlardan 9456 paketlarni tahlillashga erishgan va paketlarni filtrlash samaradorligi 84% ni tashkil etgan;

taklif etilgan usullar, algoritmlar va arxitekturalar asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi "Kibernetikada innovatsiyalar IT-parki" MChJ korporativ tarmog'ining amaliy faoliyatiga joriy etilgan (Kiberxavfsizlik markazi davlat unitar korxonasining 2024-yil fevraldagi 03-18-01/410-son ma'lumotnomasi). Sinov davomida mazkur vosita 1 soat davomida umumiy 9764 ta hodisalarni aniqlab, bulardan 546 ta hujum va 22 ta yolg'on ogohlantirishlarni aniqlashga erishdi. Shunda vositaning yolg'on ogohlantirishlar ulushi 4% ni tashkil etganligini ko'rish mumkin. Shuningdek, erishilgan ko'rsatkichlar tizimning hujumlarga qanchalik tez javob berishini va ularni blokirovkasini aniqlash, vaqt o'tishi bilan javob vaqtlarini baholash hujumlarining paydo bo'lishi tendensiyalarini va tarmoqlararo ekranlar javob vaqtlaridagi o'zgarishlarni ochib berish hamda tarmoq xavfsizlik strategiyalari va jarayonlarini takomillashtirishga imkon bergan;

tarmoq trafigining filtrlash usuli va tarmoq paketlari qoidalarini qayta ishlash vaqtini minimallashtirish algoritmlari asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi Avtomobil yo'llari Davlat qo'mitasi huzuridagi "Axborot-kommunikatsiya texnologiyalarini rivojlantirish markazi" korporativ tarmog'ining amaliy faoliyatiga joriy etilgan (O'zbekiston Respublikasi Avtomobil yo'llari Davlat qo'mitasi huzuridagi Axborot-kommunikatsiya texnologiyalarini rivojlantirish markazinnig 2024-yil apreldagi 24/32-son ma'lumotnomasi). Tadqiqot natijasida UzFirewall-next generation firewall dasturiy vositasi sezuvchanlik mezoni bo'yicha barcha joriy tarmoq anomaliyalarining taqriban 92% ini hamda aniqlik mezoni bo'yicha tarmoq anomaliyalari sifatida tasniflangan barcha hodisalarning taqriban 84% ini aniqlashga imkon bergan;

veb-resurslarni zararli botlar va shubhali paketlardan himoyalash algoritmlari asosida ishlab chiqilgan UzFirewall-next generation firewall dasturiy vositasi O'zbekiston Respublikasi Ichki ishlar vazirligi "Xavfsiz shahar" tizimlarini rivojlantirish markazi" korporativ tarmog'ining amaliy faoliyatiga tatbiq etilgan (O'zbekiston Respublikasi Ichki ishlar vazirligi "Xavfsiz shahar" tizimlarini rivojlantirish markazining 2024-yil apreldagi 03/419-son ma'lumotnomasi). Sinov davomida UzFirewall-next generation firewall dasturiy vositasi Gauss taqsimoti funksiyasi asosida tarmoq paketlari xususiyatlarini baholashda tarmoq paketlarining normal trafikka tegishlilik ehtimolligi taqriban 0,7% va hujumkor trafikka tegishlilik ehtimolligi 0,2% ni tashkil etilganligi qayd etilgan. Ushbu baholash tarmoq trafigini tasniflash usullarining samaradorligini miqdoriy baholash va ularning ish faoliyatini aniqlashga imkon bergan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 9 ta xalqaro va 10 ta respublika ilmiy-amaliy anjumanlarda muhokamadan o'tkazilgan.

Tadqiqot natijalarining e'lon qilinganligi. Dissertatsiyaning mavzusi bo'yicha jami 37 ta ilmiy ish chop etilgan, jumladan, O'zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarida 15 ta maqola, jumladan, 10 tasi xorijiy va 5 tasi respublika jurnallarida nashr etilgan hamda EHM uchun yaratilgan 3 ta dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, beshta bob,

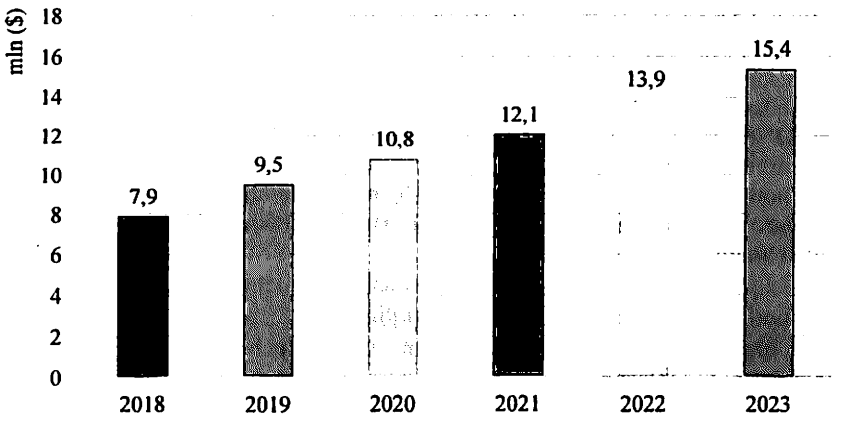
xulosa, foydalanilgan adabiyotlar ro'yxati va ilovalardan iborat. Dissertatsiya hajmi 184 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi va zarurati keltirilib, tadqiqotning O'zbekiston Respublikasi fan va texnologiyalari rivojlanishining ustuvor yo'nalishlariga mosligi ko'rsatilgan, maqsad va vazifalari belgilab olingan hamda tadqiqot obyekti va predmeti aniqlangan, olingan natijalarning ishonchliligi asoslab berilgan. Ularning nazariy va amaliy ahamiyati ochib berilgan, tadqiqot natijalarini amalga tatbiq etish ro'yxati taqdim qilingan, nashr etilgan ishlar va dissertatsiyaning tuzilishi bo'yicha ma'lumotlar keltirilgan.

Dissertatsiyaning **"Axborot-kommunikatsiya tizimlarida tarmoq trafigini himoyalash usullarining tahlili"** deb nomlanuvchi birinchi bobi axborot-kommunikatsiya tizimlarida tarmoq trafigi xavfsizligini ta'minlash usullariga, o'tkazuvchanlik qobiliyatining o'lchash usullarini tahlillash va tarmoq trafigini tasniflash hamda filtrlashning mavjud usullarini muammolariga bag'ishlangan.

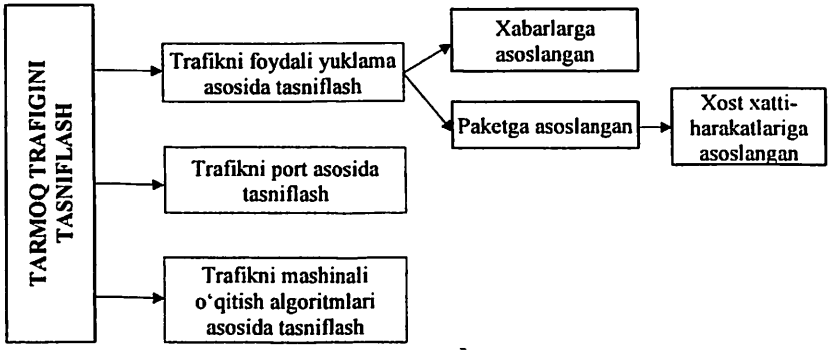
Respublikamizda raqamli iqtisodiyot tizimining shakllantirilishi va uning zamirida davlat boshqaruv organlari hamda aholi o'rtasidagi o'zaro aloqaning mustahkamlanishini tashkil etish tarmoqdan foydalangan holda amalga oshiriladi. Tarmoqdan samarali foydalanish axborotlashgan demokratik jamiyatni shakllantirishni ta'minlaydi. Bunday jamiyatda axborot almashinuv tezligi yuksaladi, axborotni yig'ish, saqlash, ishlash va ulardan foydalanish bo'yicha tezkor natijaga ega bo'linadi. Tahlil natijalariga asoslanib jahonda DDoS hujumlari soni o'sishda davom etmoqda va Cisco ma'lumotlariga ko'ra, bu o'sish 2023-yil oxiriga kelib, 2018-yilga nisbatan ikki baravar ko'proq hujumlar sodir etilganligini ko'rish mumkin. 1-rasmda 2018-2023-yillarda DDoS hujumlarining o'rtacha yillik o'sish sur'ati taqdim etilgan.



1-rasm. DDoS hujumlarining 2018-2023-yillardagi o'rtacha yillik o'sish sur'ati

Taqsimlangan axborot-kommunikatsiya tizimlariga hujumlar natijasida kelib chiqadigan tahdidlarni aniqlash va ularga javob berishning samarali usullarini talab qiladi. Eng katta muammo tanlangan tarmoq trafigi atributlari to'plamining xususiyatlari g'ayritabiiy xatti-harakatlarga ega hujumlar tufayli yuzaga keladi.

Trafikni filtrlash tizimlarini ishlab chiqish yo'nalishlaridan biri tarmoq trafigini tasniflash bo'lib, u xizmat ko'rsatish sifatini nazoratlash va kanal o'tkazuvchanligini samarali boshqarish imkonini beradi. Yondashuvlar sonining ko'payishi bilan ularni tasniflash zarurati paydo bo'ldi. Trafikni tasniflash usullari 2-rasmda keltirilgan.



2-rasm. Tarmoq trafigini tasniflash usullari

Bunda tarmoq trafigini tasniflash usullarini tahlillash asosida xost va portlarning anomal xatti-harakatlarining xarakteristikalari va foydali yuklamalari aniqlanadi. Bu esa tarmoqda xizmat ko'rsatish sifatini nazoratlash va trafikni filtrlashning yanada takomillashgan tizimini yaratish imkonini beradi.

Dissertatsiyaning **"Axborot-kommunikatsiya tizimlarida zararli trafikni aniqlash modellari"** deb nomlanuvchi ikkinchi bobida tarmoqdagi zararli trafik turlari va ularni aniqlash usullari tahlil etilgan. Tarmoq trafigida tarmoq anomaliyalari va noqonuniy harakatlarni aniqlash bosqichlarining tahlili natijasida ularni aniqlash algoritmi ishlab chiqilgan. Tarmoqdagi holatlarni boshqarish va tahlili asosida tarmoq trafigini identifikatsiyalashning axborot modeli taklif etilgan. Tarmoq trafigi tasniflagichini o'qitish hamda mashinali o'qitish usullarini qo'llagan holda DNS serverlarida zararli trafikni bartaraf etish modeli takomillashtirilgan.

Tarmoq trafigidagi anomaliyalarni aniqlash, umuman olganda, normal ma'lumotlarni u yoki bu tarzda tavsiflash, model yaratish va undan har qanday og'ishlarni anomal deb hisoblash mumkin. Bunda quyidagi jiddiy qiyinchiliklarga duch kelinadi:

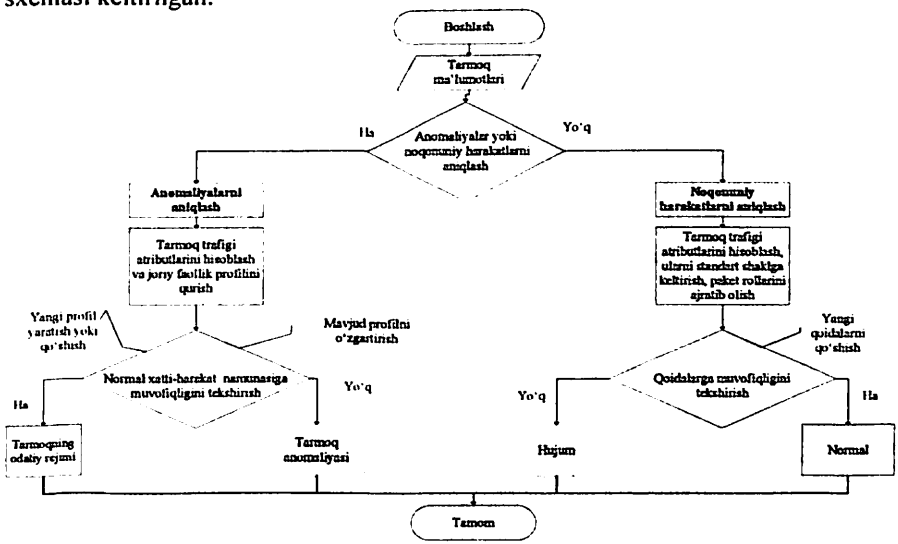
– normal nima ekanligini aniqlashdagi qiyinchilik, normal va anomal ma'lumotlar o'rtasidagi chegaraning noaniqligi;

– ma'lumotlarga normal ko'rinish berish uchun buzg'unchining o'z harakatlarini niqoblashi;

– ma'lumotlarni ishlab chiqaruvchi tizimlarning rivoji, normal tushunchasining vaqt o'tishi bilan o'zgarishiga olib keladi;

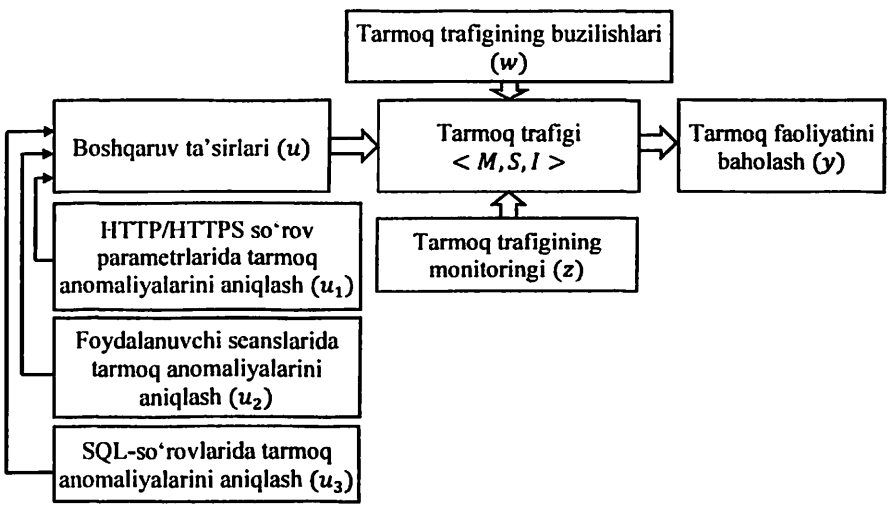
– tasniflagichlarni o'qitishda normal va anomal ma'lumotlarning mavjud emasligi.

Yuqoridagi kamchiliklarni minimallashtirish maqsadida 3-rasmda tarmoq trafigida anomaliyalar va noqonuniy harakatlarni aniqlash algoritmining blok-sxemasi keltirilgan.



3-rasm. Tarmoq trafigida anomaliyalar va noqonuniy harakatlarni aniqlash algoritmining blok-sxemasi

Bundan tashqari, tarmoq trafigini identifikatsiyalashda tarmoqni boshqarish obyekti sifatida axborot modelini yaratish maqsadga muvofiq sanaladi. 4-rasmda tarmoq trafigini identifikatsiyalashning axborot modeli taklif etilgan.



4-rasm. Tarmoq trafigini identifikatsiyalashning axborot modeli

Tarmoq trafigini identifikatsiyalashning axborot modelini quyidagicha ifodalash mumkin:

$$y = f(M, S, I, u, z, w), \quad (1)$$

bu yerda, M – tarmoq trafigini ma'lumotlari to'plami; S – tarmoq siyosati to'plami; I – tashqi ta'sirlarning ma'lumotlari to'plami; u – boshqaruv ta'sirlari; z – tarmoq trafigining monitoringi; w – tarmoq trafigining buzilishlari; y – tarmoq faoliyatini baholash.

Quyida $y = f(M, S, I, u, z, w)$ funksiyasini matematik ifodalash mumkin:

$$y = f(M, S, I, u, z, w) = [f_1(M, S, I, u, z, w), f_2(M, S, I, u, z, w), f_3(M, S, I, u, z, w), \ldots, f_r(M, S, I, u, z, w)] \quad (2)$$

Har bir qismfunksiya $y = f_i(M, S, I, u, z, w)$ quyidagicha amalga oshiriladi:

$$y = f_1(M, S, I, u, z, w) = g_1(M) + h_1(S) - \Sigma(I) + \Sigma(u) - \Sigma(z) - \Sigma(w)$$

$$y = f_2(M, S, I, u, z, w) = \alpha_2 g_2(M) + \beta_2 h_2(S) + \gamma_2 \Sigma(I) - \delta_2 \Sigma(u) - \varepsilon_2 \Sigma(z) + \varphi_2 \Sigma(w)$$

$$y = f_3(M, S, I, u, z, w) = (g_3(M) + h_3(S))\text{^}2 + \alpha_3 \Sigma(I) + \beta_3 \Sigma(u) - \gamma_3 \Sigma(z) + \delta_3 \Sigma(w)$$

$$y = f_r(M, S, I, u, z, w) = \alpha_r g_r(M) - \beta_r h_r(S) + \gamma_r \Sigma(I) - \delta_r \Sigma(u) + \varepsilon_r \Sigma(z) - \varphi_r \Sigma(w) \quad (3)$$

Ushbu ifodalarda:

– $g_i(M)$ va $h_i(S)$ –mos ravishda tarmoq trafigini ma'lumotlari to'plami M va tarmoq siyosati to'plami S ustida amallarni bajaradigan funksiyalar;

– $\Sigma(I), \Sigma(u), \Sigma(z)$ va $\Sigma(w)$ mos ravishda I, u, z va w vektorlarining elementlari yig'indisini ifodalaydi;

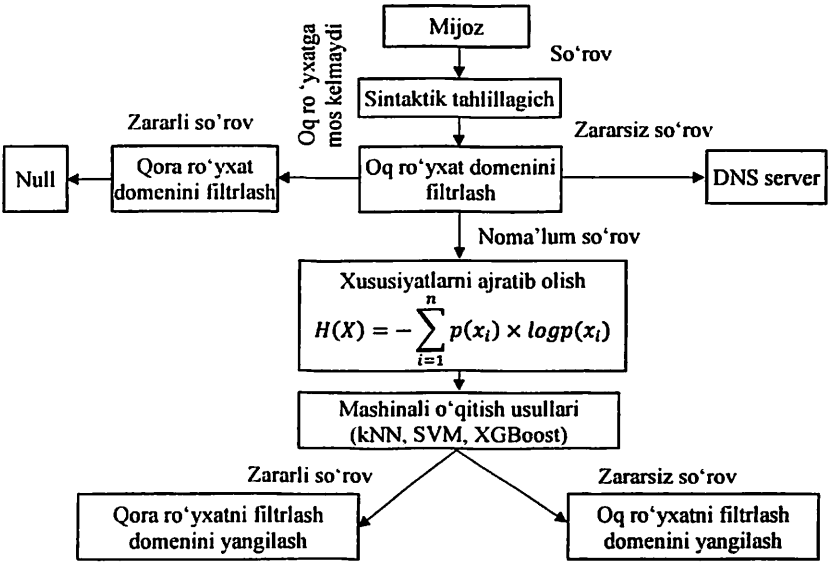
– $\alpha_i, \beta_i, \gamma_i, \delta_i, \varepsilon_i$ va φ_i –tarmoq trafigi komponentalarining o'lchovchi koeffitsiyentlari;

– matematik amallar $(+, -, \Sigma, \text{^}2)$ anomaliyalarni aniqlash tizimi talablariga asoslangan arifmetik amallar, statistik funksiyalar va boshqa tegishli matematik amallarni o'z ichiga oladi.

Umuman, taklif etilgan axborot modeli tarmoq trafigida bo'lishi mumkin tarmoq anomaliyalari va zaifliklarini aniqlash hamda axborot xavfsizligi risklarini kamaytirishga imkon beradi.

Shunday qilib, tarmoq trafigini identifikatsiyalashning axborot modeli asosida DNS serverlarida zararli trafikni bartaraf etish modelini quyidagi ikkita bosqichda amalga oshirish mumkin.

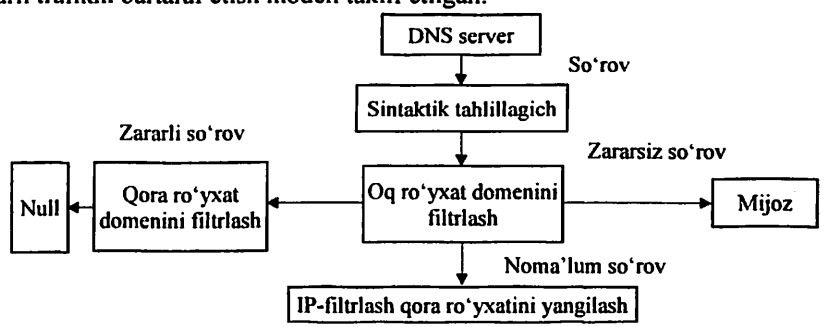
1-bosqich: 5-rasmda mijozdan serverga so'rov yuborishda DNS serverlarida zararli trafikni bartaraf etish modeli taklif etilgan. Mijozdan DNS serverga so'rovi avval domenlarning oq ro'yxatini filtrlash qismidan o'tadi. So'rov nomi ushbu qismda zararsiz deb tasniflanganida, paket qabul qiluvchi qismiga yo'naltiriladi. Aksincha, so'rov oq ro'yxatga mos kelmasa, paket domenning qora ro'yxatining filtrlash qismidan o'tadi.



5-rasm. DNS serverlarida zararli trafikni bartaraf etish modeli: mijozdan serverga so'rov .

Ushbu qismda so'rov zararli deb tasniflanganida, paket NULL qurilmasiga qaytariladi. Aksincha, so'rov domenning qora ro'yxatda mos kelmasa, paket qabul qiluvchi qismiga yo'naltiriladi. So'ngra xususiyatlarni ajratib olish qismi *qname*ni xususiyat vektorlariga aylantiradi va tasniflagich qismi so'rovni tasniflaydi. Agar tasniflash natijasi paketning zararsiz ekanligini ko'rsatsa, so'rov domenning oq ro'yxatiga qo'shiladi. Aksincha, agar natija zararli ekanligini ko'rsatsa, so'rov domenning qora ro'yxatiga qo'shilib, mashinali o'qitish usullarini qayta ishlovisiz shunday so'rovga ega bo'lgan DNS so'rovlarini blokirovka qiladi.

2-bosqich: 6-rasmda serverdan mijozga so'rov yuborishda DNS serverlarida zararli trafikni bartaraf etish modeli taklif etilgan.



6-rasm. DNS serverlarida zararli trafikni bartaraf etish modeli: serverdan mijozga so'rov

Serverdan mijozga so'rov yuborishda DNS serveridan kelayotgan DNS javobi avval domenning oq ro'yxatini filtrlash qismidan o'tadi. Agar so'rov ushbu qismda zararsiz deb tasniflangan bo'lsa, paket qabul qiluvchi qismiga yo'naltiriladi. Aksincha, so'rov oq ro'yxatda mos kelmasa, paket domenning qora ro'yxatining filtrlash qismiga o'tkaziladi. Agar so'rov ushbu qismda zararli deb tasniflangan bo'lsa, paket tizim tomonidan o'chiriladi va javob xabarida tekshiriladi. 1-jadvalda mashinali o'qitish usullaridan foydalangan holda DNS-serverlarida zararli trafikning bartaraf etish bo'yicha test natijalari keltirilgan.

1-jadval

Mashinali o'qitish usullaridan foydalangan holda DNS-serverlarida zararli trafikning bartaraf etish bo'yicha test natijalari

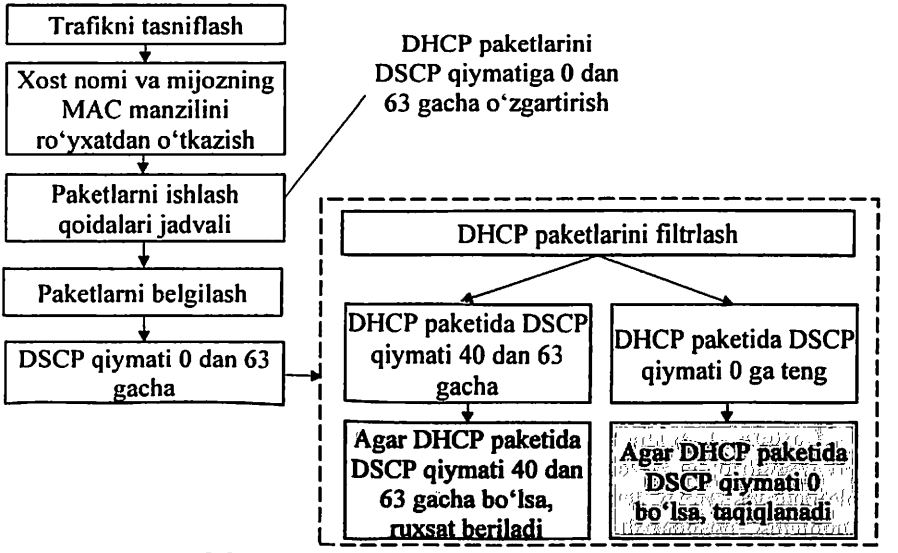
Ma'lumotlar to'plami		Mashinali o'qitish usullari	Training (80%)	Test (20%)
Soni	33925 ta satr	kNN	100	91.97
Sinfi	DrDos_DNS	SVM	100	90.94
Xususiyati	15 ta	XGBoost	100	91.92

Bu yerda ma'lumotlar to'plamini o'qitish Python dasturlash tili yordamida amalga oshirildi va test natijalari Jupyter kompilyatori orqali taqdim etilgan. Mazkur takomillashtirilgan DNS serverida zararli trafikni bartaraf etish modeli mashinali o'qitish usullari asosida mijozlardan kiruvchi, DNS serveriga bo'ladigan zararli so'rovlarni aniqlashga va DNS-trafik bilan bog'liq boshqa turdagi hujumlardan, jumladan, fishing, DDoS lardan himoya qilishga imkon beradi.

Dissertatsiyaning **"Axborot-kommunikatsiya tizimlarida tarmoq trafigini filtrlashning takomillashtirilgan usullari"** deb nomlanuvchi uchinchi bobida differensial xizmatlarning kod nuqtasi asosida tarmoqda buzg'unchilar tomonidan amalga oshirilishi mumkin bo'lgan DHCP so'rovlari kabi ma'lum tarmoq hujumlarini minimallashtirish va IP-manzilli nizolar xavfini kamaytirishga imkon beruvchi tarmoq trafigini filtrlash usuli takomillashtirilgan hamda TCP psevdo-sarlavhasini qo'shish orqali xizmat sifatini oshirish va tarmoq paketining yo'qolishini minimallashtirish usuli taklif etilgan. Server va ishchi stansiyalarning buzilish ehtimolini kamaytirish va trafik oqimlarini monitoringlash, paketlarni filtrlash qoidalarini boshqarishni soddalashtirish hamda tarmoqda suqilib kirishi mumkin bo'lgan har qanday zararli yoki istalmagan kontentni bartaraf etish usullari takomillashtirilgan.

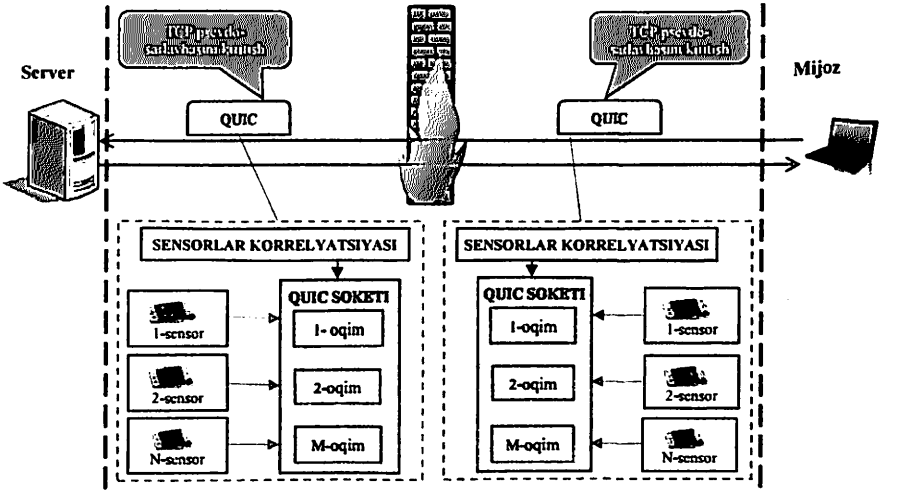
DHCP protokoli TCP/IP tarmog'ida ishlash uchun zarur bo'lgan IP-manzil va boshqa parametrlarni avtomatik ravishda olish imkonini beradi. 7-rasmda tarmoqqa ulanadigan har bir WLAN mijozi amalga oshirishi kerak bo'lgan ro'yxatga olish jarayonidan boshlab DSCP asosida DHCP paketlarini filtrlash sxemasi taklif etilgan. Bunda mazkur protokol mijoz-server modelida ishlab, foydalanuvchilarga lokal yoki Internet tarmog'i orqali ulanish imkonini beradi. DHCP protokoli har bir mijoz uchun zarur bo'lgan IP-manzilni avtomatik ravishda sozlaydi. Shuningdek, ro'yxatdan o'tgan mijozdan tashqari yuborilgan DHCP paketining DSCP qiymati 0 ga o'zgartiriladi. Keyingi bosqichda to'g'ridan-to'g'ri filtr funksiyasi har bir DHCP paketini filtrlaydi, agar DHCP paketida DSCP qiymati 40 dan 63 gacha

bo'lsa, unga paketni keyingi bosqichga o'tishiga ruxsat beriladi. Aks holda, DHCP paketi o'chirib tashlanadi.



7-rasm. DSCP asosida DHCP paketlarini filtrlash sxemasi

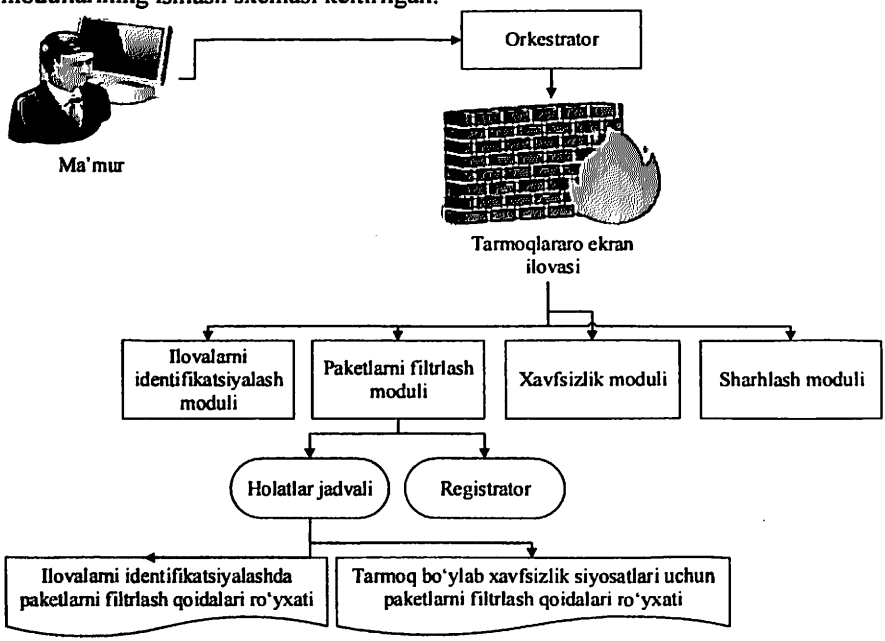
Tarmoq paketlarining yo'qolishini minimallashtirish va ularning xizmat ko'rsatish sifatini oshirish maqsadida TCP psevdo-sarlavhasidan foydalaniladi. Paket filtrlashdan o'tganidan so'ng, TCP psevdo-sarlavhasini olib tashlash orqali, uzatish paketi asl shakliga qaytadi. 8-rasmda TCP psevdo-sarlavhasini qo'shish orqali trafikni filtrlash sxemasi taklif etilgan.



8-rasm. TCP psevdo-sarlavhasini qo'shish orqali trafikni filtrlash sxemasi

TCP psevdo-sarlavha port raqamini o'zgartirish orqali ma'lumotlar almashinuvini niqoblashga, uzatiladigan tarmoq paketlarining kechikishini boshqarishga va portlarni keng diapazondan tasodifiy tanlaydigan protokollar uchun portlarni o'zgartirishga imkon beradi. QUIC protokoli yordamida paketlarni uzatishda har bir oqim, sensorni alohida obyekt sifatida ko'rib chiqadi. Sensorlar soniyada bir necha ko'rsatkichlarni ta'minlanganliklari sababli, har bir sensor uchun nafaqat turli oqimlarni, balki har bir obyekt uchun turli oqimlarni ham qo'llash taklif etiladi. Oqimga yuborilgan barcha paketlar tan olinsa, oqim yangi obyekt uchun qayta ishlatilishi mumkin. Aksincha, agar oqim paket yo'qolishi sababli blokirovkalangan va ma'lumotlar eskirgan bo'lsa, jo'natuvchi qabul qiluvchiga ushbu oqimdan olingan barcha mavjud tartibsiz ma'lumotlarni o'chirib tashlashni va oqimni qayta o'rnatish uchun kadr yuboradi. Bir necha sensorlar QUIC soketiga ma'lumotlarni yozib boradi va sensorlar o'rtasida korrelyatsiya matritsasini ta'minlaydi. Shunday qilib, taklif etilgan usul TCP psevdo-sarlavha port raqamini o'zgartirish orqali ma'lumotlar almashinuvini niqoblashga, uzatiladigan tarmoq paketlarining kechikishini boshqarishga imkon beradi.

Dasturiy ta'minot bilan aniqlanadigan tarmoq (SDN) tarmoqni aqlli va markazlashtirilgan tarzda boshqarish imkonini beradi. Bu operatorlarga tarmoqda ishlatiladigan asosiy texnologiyadan qat'iy nazar, butun tarmoqni izchil va har tomonlama boshqarish imkonini beradi. Shunday qilib, tarmoq trafigining xavfsizligini oshirishga imkon beruvchi SDN tarmoqlarida trafikni filtrlashni amalga oshirish usuli takomillashtirilgan. 9-rasmda paketlarni filtrlash modullarining ishlash sxemasi keltirilgan.



9-rasm. Paketlarni filtrlash modullarining ishlash sxemasi

Taklif etilgan sxemada tarmoqlararo ekran funksiyasi o'zaro ta'sir qiluvchi to'rtta modul yordamida amalga oshiriladi: ilovani identifikatsiyalash moduli, paketlarni filtrlash moduli, xavfsizlik va sharhlash modullari. Taklif etilgan sxema modullarining amalga oshirilishi natijasida ko'rish mumkinki, SDN tarmoqlarida trafikni filtrlashni amalga oshirish usuli trafik oqimlarini nazorat etishga, xavfsizlikni boshqarishni soddalashtirishga va har qanday istalmagan kontentning bartaraf etishga imkon beradi.

Dissertatsiyaning **"Axborot-kommunikatsiya tizimlarida shubhali tarmoq paketlarini aniqlash va bartaraf etish algoritmlari"** deb nomlanuvchi to'rtinchi bobida trafik xatti-harakatlariga muvofiq qoidalar harakatlarini o'zgartirish, tarmoq paketlarida risklarni minimallashtirish hamda tarmoq paketlarini qabul yoki rad etishda qoidalarning eng yuqori ustuvorligini aks ettirish algoritmlari ishlab chiqilgan. Tarmoqlararo ekrandagi tugunlar soni ortishi bilan tarmoq paketlari qoidalarini ishlash vaqtini kamaytirish, paketlarni to'lib-toshishi va IP-Spoofing hujumlarini minimallashtirishga imkon beruvchi filtrlash qoidalari algoritmlari optimallashtirilgan. Veb-resurslarni zararli botlardan himoya qilish hamda ko'p faktorli trafik tahlili asosida mavjud va yangi veb-hujumlarni bartaraf etish algoritmi ishlab chiqilgan. Giperhavola funksiyalaridan foydalanish hisobida veb-sahifalarning qonuniyligini tekshirish va domenlarni soxta fishing hujumlaridan hamda onlayn tahdidlar va nol hujumlaridan himoya qilish algoritmi taklif etilgan.

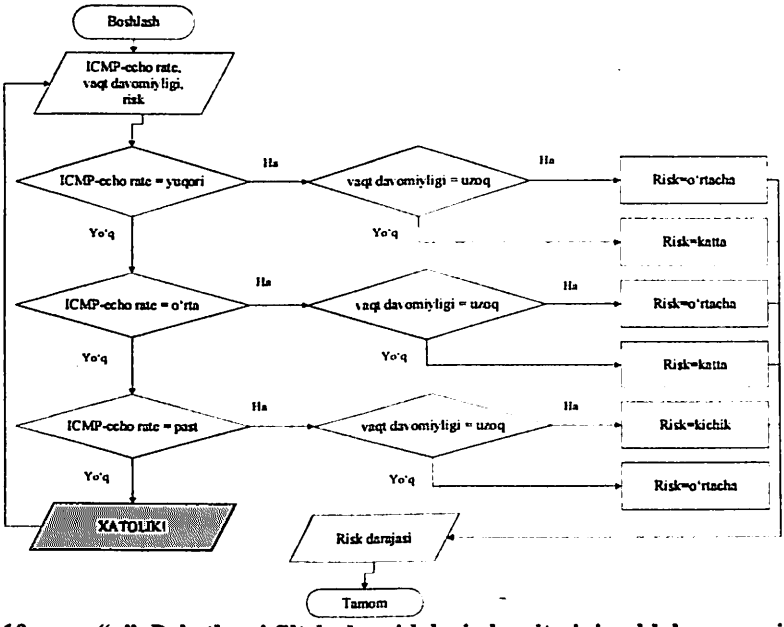
Petri noravshan tarmog'i - noravshan mantiq va Petri tarmoqlarining birikmasi. Petri noravshan tarmog'i tizim holati haqidagi noaniq bilimlarni ifodalash vositasi bo'lib, noaniq hodisa va harakat qoidalarini tavsiflash imkoniyatiga ega. Petri noravshan tarmog'ining modeli $N_f(P,T,D,I,\alpha,\beta)$ to'plami sifatida tavsiflanadi. Petri noravshan tarmog'idan tarmoqlararo ekran orqali paketlar harakatini noravshan mantiqiy boshqarishni tasvirlashda grafik usul sifatida foydalanadi va quyidagi ifoda yordamida tavsiflanadi:

$$f: U \subset \bigcup_{i=1}^{n} (R_n \cap V), \quad (4)$$

bu yerda, $U = U_1 \times U_2$ –kiruvchi fazo; V – chiquvchi fazo; R –risk darajasi.

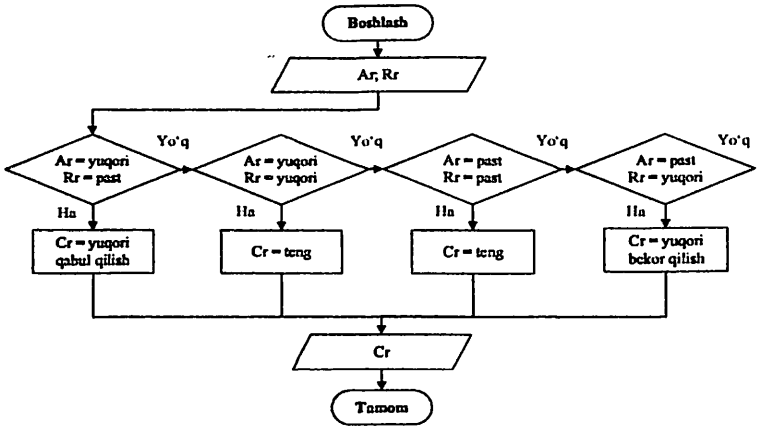
Birinchi daraja: noravshan filtrlash. Bu daraja IP-manzil, paket vaqti va protokol turi, imitatsiya va paketlarni kuzatish kabi har bir paket bilan bog'liq ma'lumotlar asosida barcha kiruvchi paketlarni ushlab olish va tasniflashga asoslangan. Paket Petri noravshan tarmog'i orqali token bilan ifodalanadi va paketning ishlashi, bir joydan ikkinchi joyga ko'chirishi uchun Petri noravshan tarmog'i mas'ul hisoblanadi. 10-rasm "a" da paketlarni filtrlash qoidalari algoritmining blok-sxemasi taqdim etilgan.

Ikkinchi daraja: noaniq filtrlash. Odatda, har bir tarmoqlararo ekranda u bilan bog'langan ikkita paketlar to'plami mavjud: tarmoqlararo ekran tomonidan qabul qilinadigan paketlar to'plami va tarmoqlararo ekran tomonidan bekor qilingan paketlar to'plami. 10-rasm "b" da paketlarni filtrlash qoidalari algoritmining blok-sxemasi taklif etilgan. Bunday holda, ikkita kirish va bitta chiqishga ega bo'lgan noravshan mantiq qo'llaniladi.



10-rasm "a". Paketlarni filtrlash qoidalari algoritmining blok-sxemasi (birinchi daraja: noravshan filtrlash)

Tarmoq paketlarini qabul qilish tezligi A_r va bekor qilish tezligi $R_r$ni tavsiflash uchun ikkita noravshan o'zgaruvchilar, jumladan "past" va "yuqori", ishlatiladi. Noravshan mantiqning natijasi trafikda bekor qilish va qabul qilish tezligini tavsiflovchi C_r hisoblangan miqdori bo'lib, uchta noravshan o'zgaruvchilar, jumladan yuqori bekor qilish darajasi, teng va yuqori qabul qilish darajasi bilan tavsiflanadi.



10-rasm "b". Paketlarni filtrlash qoidalari algoritmining blok-sxemasi (ikkinchi daraja: noravshan filtrlash)

Paketlarni filtrlash qoidalari algoritmlarini optimallashtirish. Quyida paketlarni filtrlash qoidalari algoritmlarining paketlarni ortiqchaligi kriteriyasi bo'yicha optimallashtirish amallari amalga oshirilgan. Har bir ortiqcha qoida trafik tahlilining murakkabligini va narxini oshiradi, shuning uchun ularning sonini kamaytirish tizimning barqaror ishlashiga imkon yaratadi.

Faraz qilaylik,

$Min \sum_{i=1}^{n} D_i \times x_i$ –maqsadli funksiya bo'lsin.

Bu yerda, $D_i - i$ qoidalari uchun ortiqchalik darajasi; $x_i - i$ qoidasining foydalanilishi (1) yoki foydalanmasligini (0) belgilovchi o'zgaruvchilar; n –paketlarni filtrlash qoidalarining soni.

Paketlarni filtrlash qoidalari ortiqchaligini minimallashtirish quyidagi chegaralar asosida belgilanadi:

1. $\sum_{i=1}^{n} a_{ij} \times x_i \geq b_j$ – xavfsizlik cheklovlari;
2. $\sum_{i=1}^{n} r_{ij} \times x_i \geq R_j$ – resurslar cheklovlari.

Bu yerda, $a_{ij} - i$ qoidaning xavfsizlik cheklovi j ga ta'sir qiluvchi matritsa elementi; $b_j - j$ qoidaning xavfsizlik cheklovi uchun minimal talab qilinadigan qiymat; $r_{ij} - i$ qoidaning resurs j ga ta'sir qiluvchi matritsa elementi; $R_j - j$ resurs uchun ajratilgan maksimal qiymat. Trafikni filtrlash qoidalari algoritmlarini optimallashtirish natijasida tarmoqlararo ekrandagi tugunlar soni ortishi bilan tarmoq paketlari qoidalarini ishlash vaqtini kamaytirish, paketlarni to'lib- toshishi va ortiqchaligi hamda tarmoqda bo'ladigan IP-Spoofing hujumlarini minimallashtirishga erishildi. 2-jadvalda paketlarni filtrlash qoidalarida ortiqchalikni aniqlash kriteriyasining darajalari bo'yicha optimallashtirish natijalari taqdim etilgan.

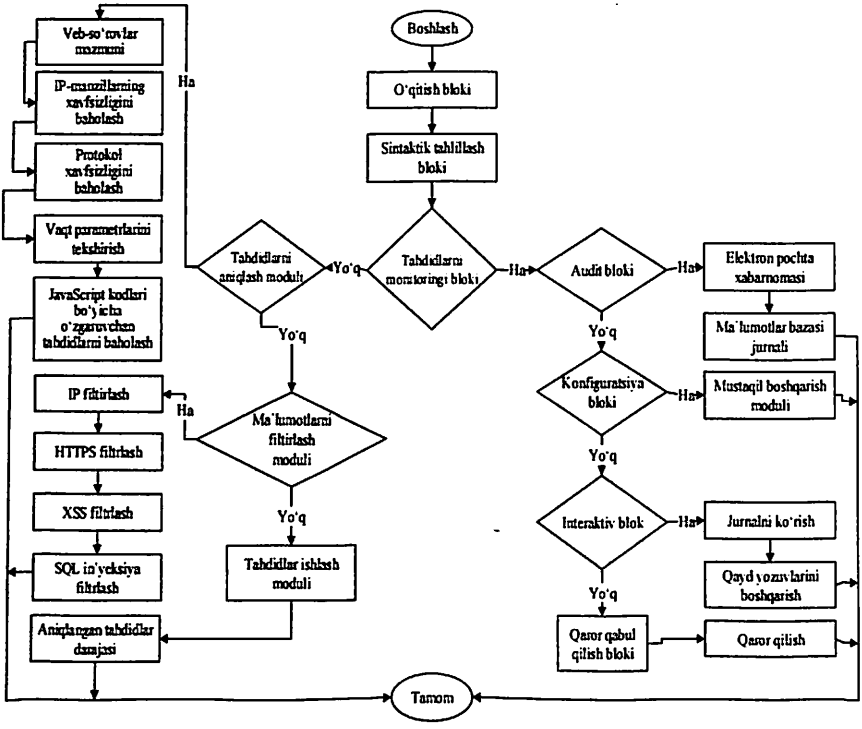
2-jadval

Paketlarni filtrlash qoidalarida ortiqchalikni aniqlash kriteriyasining darajalari bo'yicha optimallashtirish natijalari

№	Algoritm nomi	Optimallashtirish natijalari $Min \sum_{i=1}^{n} D_i \times x_i$
1.	Qoidalarni zichlash	5.4%
2.	Qoidalarni taqsimlash	4.7%
3.	Metaqoidalarni generatsiyalash	7.1%
4.	O'zaro qarama-qarshi bo'lmagan qoidalarni generatsiyalash	5.3%

Internetdan foydalanuvchilar soni ortishi bilan trafikni veb-filtrlash ahamiyati ortib bormoqda. Trafikni veb-filtrlash teskari proksi-serverning bir turi bo'lib, shubhali trafikni aniqlash orqali veb-serverni mijozga ko'rsatilishidan himoya qiladi. 11-rasmda veb-hujumlardan himoyalashda veb-resurslarni filtrlash algoritmininig blok-sxemasi taqdim etilgan. Shuningdek, shubhali paketlarni aniqlashda tarmoq paketlarining manba va maqsad IP-manzili, port, protokol, paket

o‘lchami hamda har bir paket uchun uning shubhali yoki shubhali emasligini ko‘rsatuvchi sinf belgilarini o‘z ichiga olgan ma’lumotlar to‘plamidan foydalaniladi.



11-rasm. Veb-hujumlardan himoyalashda veb-resurslarni filtrlash algoritmining blok-sxemasi

Bu to‘plamni quyidagicha tavsiflash kerak bo‘ladi:

Paket xususiyatlari. Har bir tarmoq paketi bir qator xususiyatlar bilan tavsiflanadi:

$$X = \{x_1, x_2, \dots, x_n\}, \quad (5)$$

bu yerda,

x_i –paketning o‘ziga xos xususiyatini ifodalaydi, masalan, IP-manzil, port, protokol va b.

Sinf belgilari. Agar $y = 1$ bo‘lsa paket shubhali bo‘lsin, agar $y = 0$ bo‘lsa normal paket bo‘lsin, ya’ni

$$F(x) = \begin{cases} y = 1, & paket\ shubhali\ hisoblanadi \\ y = 0, & paket\ zararli\ hisoblanadi \end{cases} \quad (6)$$

Shubhali paketlar ulushini aniqlashda paket xususiyatlari va sinf belgilari asosida logistik regressiya usulidan foydalaniladi, ya’ni

$$LR_v(X) = \frac{1}{1 + e^{-vx}}, \quad (7)$$

bu yerda, v –vektor parametrlari hisoblanadi.

Mazkur algoritm tizim veb havolaning zararsizligini tekshirganidan so'ng, agar sayt fishing bo'lsa, foydalanuvchini ogohlantiradi, agar sayt zararsiz bo'lsa, tizimning oq ro'yxatidagi domenini yangilaydi.

Dissertatsiyaning **"Trafikni filtrlashning dasturiy vositasi samaradorligini baholash va amaliyotga tatbiq etish natijalari"** deb nomlanuvchi beshinchi bobida standart filtrlash vositalari tomonidan o'tkazib yuborilgan tarmoq paketlarini aniqlash, ajratish va blokirovkalash, paketlarni filtrlash qoidalari sonini optimallashtirish orqali yolg'on xabarlarni minimallashtirish hamda DDoS hujumlari so'rovlarini blokirovkalash va tizimga zararli kodlarni kirishini minimallashtirishga imkon beruvchi UzFirewall-next generation firewall dasturiy vositasi ishlab chiqilgan. Mazkur dasturiy vosita O'zbekiston Respublikasining soha korxonalari axborot markazlarida amaliyotga tatbiq etilgan va tarmoq trafigini filtrlash, filtrlash qoidalarini optimallashtirish, tarmoq anomaliyalarini aniqlash, yolg'on ogohlantirishlarni aniqlash hamda tarmoq tahdidlarini minimallashtirish bo'yicha natijalar qayd etilgan.

Tashkilotning axborot resurslarini to'liq himoya qilishni ta'minlashda, dasturiy vositalar yechimlaridan foydalanish talab etiladi. Bu borada taklif etilgan UzFirewall-next generation firewall dasturiy vositasi ilg'or yechim sifatida o'zining samaradorligini va undan muntazam foydalanish uchun yetarli darajada xavfsizligini ko'rsatdi. Tarmoqlararo ekranlar samaradorligini, xususan, UzFirewall-next generation firewall dasturiy vositasining mavjudlari bilan baholash 3, 4 va 5-jadvallarda qayd etilgan.

Ijobiy bashoratlash qiymati mezoni-Positive Predictive Value (PPV). Mazkur mezon to'g'ri tasniflangan paketlar sonini aniqlashga imkon beradi. 3-jadvalda tarmoqlararo ekranlarning samaradorligini PPV mezoni bo'yicha baholash taqdim etilgan.

3-jadval

Tarmoqlararo ekranlarning samaradorligini PPV mezoni bo'yicha baholash

Vositalar	$PPV = \frac{\text{To'g'ri tasniflangan paketlar soni}}{\text{Paketlarning umumiy soni}} \times 100$	%
ZyWALL ATP200	$PPV = \frac{1630}{1700} \times 100$	95,8
ZoneAlarm Free Firewall 15.8.213.19411	$PPV = \frac{1627}{1700} \times 100$	95,7
UzFirewall-next generation firewall	$PPV = \frac{1669}{1700} \times 100$	98,1
TinyWall	$PPV = \frac{1586}{1700} \times 100$	93,2
PrivateFirewall 7.0.30.3	$PPV = \frac{1591}{1700} \times 100$	93,5

To'liqlik (Recall) mezoni. To'liqlik mezoni trafikda barcha zararli paketlarini aniqlash qobiliyatini o'lchashga imkon beradi. 4-jadvalda tarmoqlararo ekranlarning samaradorligini to'liqlik mezoni bo'yicha baholash taqdim etilgan.

4-jadval

Tarmoqlararo ekranlarning samaradorligini to'liqlik mezoni bo'yicha baholash

Vositalar	To'liqlik $= \frac{\text{To'g'ri tasniflangan zararli paketlar soni}}{\text{Zararli paketlarning umumiy soni}} \times 100$	%
ZyWALL ATP200	$To'liqlik = \frac{673}{700}$	96,1
ZoneAlarm Free Firewall 15.8.213.19411	$To'liqlik = \frac{671}{700}$	95,8
UzFirewall-next generation firewall	$To'liqlik = \frac{686}{700}$	98,0
TinyWall	$To'liqlik = \frac{639}{700}$	91,2
PrivateFirewall 7.0.30.3	$To'liqlik = \frac{640}{700}$	91,4

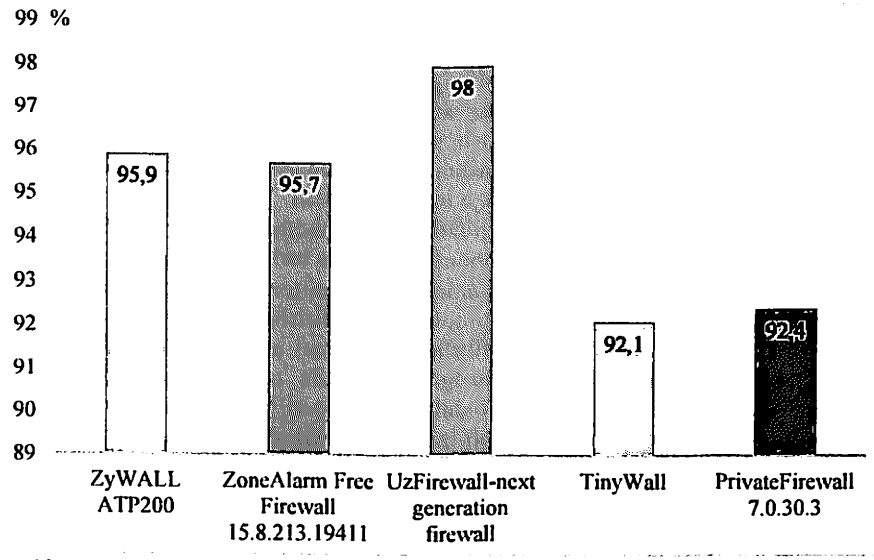
F1-o'lchov (F1-Score) mezoni. 5-jadvalda tarmoqlararo ekranlarning samaradorligini F1-o'lchov mezoni bo'yicha baholash taqdim etilgan.

5-jadval

Tarmoqlararo ekranlarning samaradorligini F1-o'lchov mezoni bo'yicha baholash

Vositalar	$F1 = 2 \times \frac{\text{PPV} \times \text{Recall}}{\text{PPV} + \text{Recall}}$	%
ZyWALL ATP200	$F1 = 2 \times \frac{95{,}8 \times 96{,}1}{95{,}8 + 96{,}1}$	95,9
ZoneAlarm Free Firewall 15.8.213.19411	$F1 = 2 \times \frac{95{,}7 \times 95{,}8}{95{,}7 + 95{,}8}$	95,7
UzFirewall-next generation firewall	$F1 = 2 \times \frac{98{,}1 \times 98}{98{,}1 + 98}$	98,0
TinyWall	$F1 = 2 \times \frac{93{,}2 \times 91{,}2}{93{,}2 + 91{,}2}$	92,1
PrivateFirewall 7.0.30.3	$F1 = 2 \times \frac{93{,}5 \times 91{,}4}{93{,}5 + 91{,}4}$	92,4

12-rasmda tarmoqlararo ekranlarning samaradorligini F1-o'lchov mezoni bo'yicha baholash diagrammasi taqdim etilgan.



12-rasm. Tarmoqlararo ekranlarning samaradorligini F1-o'lchov mezoni bo'yicha baholash diagrammasi

Yuqoridagi baholash mezonlari asosida tarmoqlararo ekranlar ustida amalga oshirilgan qiyosiy tahlillar natijasiga ko'ra taklif etilgan UzFirewall-next generation firewall dasturiy vositasi boshqa tarmoqlararo ekranlarga nisbatan yuqori natijalarni qayd etganligi bilan izohlanadi.

XULOSA

"Axborot-kommunikatsiya tizimlarida tarmoq trafigini filtrlashning usuli va vositalari" mavzusidagi dissertatsiya ishi bo'yicha olib borilgan tadqiqot natijalari asosida quyidagi xulosalar taqdim etildi:

1. Tarmoq trafigini identifikatsiyalashning axborot modeli taklif etilgan. Natijada tarmoq trafigida bo'lishi mumkin bo'lgan zaifliklar va HTTP/HTTPS hamda SQL so'rovlari parametrlarida anomaliyalarni aniqlash orqali tashqi tahdidlar ta'sirini minimallashtirishga va identifikatsiyalashga erishilgan.

2. Mashinali o'qitish usullari asosida DNS serverlarida zararli trafikni bartaraf etish modeli takomillashtirilgan. Natijada mijozlardan kiruvchi DNS so'rovlarini tahlillash, aniqlash va blokirovkalash, qora va oq ro'yxatlar domenlarini yangilab borish hamda DNS-trafik bilan bog'liq boshqa turdagi, jumladan, fishing, DDoS hujumlaridan himoyalanishga imkon yaratilgan.

3. Differensial xizmatlarning kod nuqtasi asosida tarmoq trafigini filtrlash usuli taklif etilgan. Natijada tarmoqda buzg'unchilar tomonidan amalga oshirilishi mumkin bo'lgan DHCP so'rovlari kabi ma'lum tarmoq hujumlarini minimallashtirish, IP-manzilli nizolar xavfini kamaytirish hamda DHCP paketlarining maksimal sonini cheklash qoidasini o'rnatish orqali, DHCP

serverining ortiqcha yuklanishini bartaraf etishga erishilgan.

4. TCP psevdo-sarlavhasini qo'shish orqali tarmoq paketlarining yo'qolishini minimallashtirish va ularning xizmat ko'rsatish sifatini oshirish usuli taklif etilgan. Natijada tarmoq trafigi oqimini normallashtirish, tarmoqni ishdan chiqishi holatlarini minimallashtirish, TCP psevdo-sarlavha port raqamini o'zgartirish orqali ma'lumotlar almashinuvini niqoblash va uzatiladigan tarmoq paketlarining kechikishini boshqarishga imkon berilgan.

5. Tarmoq trafigida portni taqillatish usuli takomillashtirilgan. Natijada bir vaqtning o'zida autentifikatsiya urinishlari bo'lganida turli uzunlikdagi taqillatishlar ketma-ketligini qo'llash orqali portni aniqlash vaqtini tezlashtirishga hamda server va ishchi stansiyalar buzilishining ehtimolini kamaytirishga erishilgan.

6. Orkestrator va paketlarni filtrlash modullari asosida SDN tarmoqlarida trafikni filtrlash usuli takomillashtirilgan. Natijada tarmoq trafigi oqimlarini monitoringlash, paketlarni filtrlash qoidalarini boshqarishni soddalashtirish hamda tarmoqda suqilib kirishi mumkin bo'lgan har qanday zararli yoki istalmagan kontentni bartaraf etishga imkon yaratilgan.

7. Ikki darajali noravshan paketlarni filtrlash algoritmlari ishlab chiqilgan. Natijada tarmoq trafigi xatti-harakatlariga muvofiq tarmoq paketlarida qoidalar harakatlarini o'zgartirish va risklarni minimallashtirish, noravshan filtrlashni qo'llash orqali paketlarni filtrlash unumdorligini oshirish hamda tarmoq paketlarini qabul yoki rad etishda qoidalarning eng yuqori ustuvorligini aks ettirishga erishilgan.

8. Tarmoq trafigida filtrlash qoidalari algoritmlari optimallashtirilgan. Natijada tarmoqlararo ekrandagi tugunlar soni ortishi bilan tarmoq paketlari qoidalarining ishlashi vaqtini kamaytirish, paketlarni to'lib-toshishi va tarmoqda bo'ladigan IP-Spoofing hujumlarini minimallashtirish imkoni yaratilgan hamda paketlarni ortiqchalik kriteriyasining darajalari bo'yicha optimallashtirish umumiy 5,62% ni tashkil etilganligi qayd etilgan;

9. Veb-so'rovlarni ishlash bloklari asosida veb-resurslarni filtrlash va tarmoq trafigidagi shubhali paketlarni aniqlash algoritmlari ishlab chiqilgan. Natijada veb-resurslarni zararli botlardan himoyalash, veb-sahifalarni haqiqiyligini tekshirish va domenlarni onlayn tahdidlar va soxta fishing hujumlaridan himoya qilishga erishilgan.

10. UzFirewall-next generation firewall dasturiy vositasi soha korxonalarining axborot markazlariga joriy etish natijalariga ko'ra, Kerio Control 8.3.0 dasturiy vositasiga nisbatan ma'lumotlarning uzatishning tezligi 2.7 marta tezroq ishlashiga, tarmoq hujumlarini 96% aniqlik bilan bartaraf etishga, shubhali paketlarni blokirovkalash bo'yicha 95% samarali ishlashiga, tarmoq paketlarini 84% samarali filtrlashiga imkon bergan hamda tarmoq paketlari xususiyatlarini baholashda tarmoq paketlarining normal trafikka tegishlilik ehtimolligi taqriban 0,7% va hujumkor trafikka tegishlilik ehtimolligi 0,2% ni tashkil etilganligi qayd etilgan.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.02
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ГУЛОМОВ ШЕРЗОД РАЖАБОЕВИЧ

МЕТОДЫ И СРЕДСТВА ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

05.01.05 - Методы и системы защиты информации. Информационная безопасность

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ТЕХНИЧЕСКИХ НАУК (DSc)**

Ташкент-2024

Тема диссертации доктора технических наук (DSc) зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан за № B2024.1.DSc/T770

Диссертация выполнена в Ташкентском университете информационных технологий имени Мухаммада ал-Хоразмий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещён на веб-сайте Научного совета (www.tuit.uz) и на информационно-образовательный портале (www.ziyonet.uz) «ZiyoNet».

Научный консультант:	**Каримов Маджит Маликович,** доктор технических наук, профессор
Официальные оппоненты:	**Рахматуллаев Марат Алимович** доктор технических наук, профессор
	Керимов Камил Фикратович доктор технических наук, доцент
	Курязов Давлатер Матякубович доктор физико-математических наук
Ведущая организация:	**Национальный университет Узбекистана имени Мирзо Улугбека**

Защита диссертации состоится 29 июня 2024 года в 11:00 часов на заседании Научного совета DSc.13/30.12.2019.T.07.02 при Ташкентском университете информационных технологий. (Адрес: 100084, г.Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий (регистрационный номер № 317). (Адрес: 100084, г.Ташкент, ул. Амир Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан 21 июня 2024 года.

(протокол рассылки № 13 от 21 июня 2024 года)

Б.Ш. Махкамов
Председатель Научного совета по присуждению ученых степеней, доктор экономических наук, профессор

М.С. Санткамолов
Ученый секретарь Научного совета по присуждению ученых степеней, доктор экономических наук, доцент

С.К. Ганиев
Председатель Научного семинара при Научном совете по присуждению ученых степеней, доктор технических наук, профессор

ВВЕДЕНИЕ (аннотация докторской диссертации (DSc))

Актуальность и востребованность темы диссертации. В результате стремительного развития и внедрения информационно-коммуникационных систем по всему миру, наряду с возможностями, предоставляемыми пользователям, увеличивается доля угроз и атак в сетях. По результатам проведенного анализа статистических данных ИТ-компаний мира можно сделать вывод, что уровень реализации DDoS-атак в информационно-коммуникационных системах остается высоким. В частности, по данным специалистов компании CloudFlare, во втором квартале 2023 года объем HTTP DDoS-атак увеличился на 15% по сравнению с первым кварталом, а в третьем квартале наблюдается рост этого показателя на 65%[1]. Отдельно следует отметить, что практически все виды атак вызваны недостатками конфигурации систем обнаружения вторжений и межсетевых экранов, а также отсутствием достаточного количества модулей защиты от атак. В США, Китайской Народной Республике, Российской Федерации, Великобритании, Ирландии, Германии, Италии, Испании, Бразилии, Японии, Южной Корее и других странах мира все большее значение приобретают оптимизация сетевых пакетных правил, совершенствование информационных моделей обнаружения и выявления аномалий в сетевом трафике, обнаружение и предотвращение сетевых атак, разработка методов и алгоритмов фильтрации сетевого трафика.

Согласно мировому опыту, проводятся научные и практические исследования, направленные на разработку моделей, методов и алгоритмов фильтрации трафика, основанные на обнаружении и предотвращении сетевых атак в информационно-коммуникационных системах, методов обнаружения аномалий в сетевых пакетах и средств обнаружения подозрительных пакетов. В результате исследований по разработке методов и средств фильтрации сетевого трафика в информационно-коммуникационных системах достигнуты ряд научных результатов, в том числе: разработаны прокси-серверы данных и когнитивные межсетевые экраны (Массачусетский технологический институт, США); усовершенствованы возможности модели записей межсетевого экрана COAST за счет добавления функции преобразования блоков передачи и функции сопоставления значений атрибутов (Чжэцзянский Университет, Китайская Народная Республика); разработан межсетевой экран нового поколения Next Generation Firewall, выполняющий классификацию протоколов и сервисов, мониторинг и блокировку трафика на различных уровнях модели OSI от уровня сети до уровня приложений (компания TexArgos, Российская Федерация); разработаны алгоритмы доступа и отказа для эффективной работы сетевой безопасности и доказана эффективность алгоритма на базе платформы моделирования сети mininet (Университет Джона Хопкинса, США); на основе оптимизации правил фильтрации пакетов разработана стратегия защиты, снижающая количество фишинговых атак и

[1] https://blog.cloudflare.com/ddos-threat-report-2023-q3/

система Hopeypot (Государственный университет Айдахо, США); разработан метод, обеспечивающий безопасность информации в заголовках пакетов путем установки межсетевых экранов между маршрутизаторами Networks-on-Chip (NoC) (Мюнхенский технический университет, Германия и Университет Сан-Паулу, Бразилия). В связи с этим одной из актуальных задач считается оптимизация правил фильтрации пакетов, реализация методов фильтрации трафика в SDN-сетях, совершенствование и разработка алгоритмов обнаружения вредоносного трафика на рабочих станциях и архитектур фильтрации веб-ресурсов. Для решения этих проблем необходимо выявить, оценить ряд новых типов атак, а также научно обосновать усовершенствованные методы и средства их предотвращения.

Органами государственного и хозяйственного управления, государственной власти проводится большая работа, направленная на совершенствование методов и средств фильтрации сетевого трафика в процессе защиты сети от внутренних и внешних атак в масштабах нашей республики. В Стратегии развития Нового Узбекистана на 2022-2026 годы определены задачи по "определению основных направлений обеспечения кибербезопасности Интернет-пространства доменной зоны «UZ» и комплексных задач по защите систем электронного правительства[2], энергетики, цифровой экономики и других сфер, связанных с важной информационной инфраструктурой". При решении этих задач важны разработка и совершенствование моделей обнаружения аномалий сетевых пакетов, методов и алгоритмов фильтрации сетевых пакетов, а также средств предотвращения подозрительных пакетов в информационно-коммуникационных системах.

В определенной степени данное диссертационное исследование служит реализацией решений указов и постановлений Президента Республики Узбекистан, в частности, №УП-60 "О стратегии развития нового Узбекистана на 2022-2026 годы" от 28 января 2022 года, №ПП-357 "О мерах по поднятию на новый уровень сферы информационно-коммуникационных технологий в 2022-2023 годах" от 22 августа 2022 года, №УП-4452 "О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты" от 14 сентября 2019 года, №УП-5349 "О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций" от 19 февраля 2018 года и №ПП-4024 "О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты" от 21 ноября 2018 года, а также задач, поставленных в других нормативно-правовых актах, связанных с этой деятельностью.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в рамках приоритетного направления развития науки и технологий республики

[2] O'zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi PF-60-son «2022 - 2026 yillarga mo'ljallangan Yangi O'zbekistonning Taraqqiyot strategiyasi to'g'risida» gi Farmoni

IV. «Развитие информатизации и информационно-коммуникационных технологий».

Обзор научных исследований по теме диссертации[3]. Научные исследования направленные на разработку методов и средств фильтрации сетевого трафика в информационно-коммуникационных системах проводятся в самых передовых и ведущих научно-исследовательских институтах, исследовательских центрах и университетах мира, в числе которых Sababa Security (Италия), Cybergamp (Испания), Geedge Networks (Китайская Народная Республика), Оксфордский университет (Великобритания), Имперский колледж Лондона (Великобритания), Массачусетский технологический институт (США), Беркли, Калифорнийский университет (США), Университет Джонса Хопкинса (США), Университет Северной Джорджии (США), Государственный университет Айдахо (США), Дублинский университет (Ирландия), Мюнхенский технический университет (Германия), Чжэцзянский Университет (Китайская Народная Республика), Московский государственный технический университет им. Н.Э. Баумана (Российская Федерация), TexArgos (Российская Федерация), Южнокорейский институт науки и технологий (Южная Корея), Токийский технологический институт (Япония), Университет Васэда (Япония), Университет Сан-Паулу (Бразилия), а также в научно-исследовательских институтах, исследовательских центрах и университетах нашей республики, среди которых Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, Национальный университет Узбекистана имени Мирзо Улугбека, Университет Инха в Ташкенте, Научно-исследовательский институт развития цифровых технологий и искусственного интеллекта, ГУП «Центр кибербезопасности», Центр научных, технических и маркетинговых исследований «UNICON.UZ».

Степень изученности проблемы. Денис Салопек проводил исследования по разработке гибридного аппаратно-программного обеспечения для фильтрации пакетов в реальном времени. Такие ученые, как Лианг Ли, Гуан-Ю Лин, Яв Чунг Чен проводили исследования по разработке алгоритмов быстрого обнаружения конфликтов для многомерной фильтрации пакетов. Исследователями Луис А.Трежо, Виктор Ферман, Мигуел Ангел Медина Перез, Фернандо Мигуел Арредондо Жиакенти, Раул Монрой, Хосе Эмануел Рамирез-Маркуез проведены научные исследования по применению визуальных платформ для обнаружения аномалий посредством машинного обучения и защиты серверов доменных имен верхнего уровня от DDoS-атак: DNS-ADVP. Х. Алимохаммади, М. Ахмади, провели научные исследования по общим подходам сегментации пакетов SDN на основе нескольких полей без символов Джокера, и они до сих пор продолжаются возглавляемыми ими научными школами. Кроме того, в компаниях и организациях Palo Alto Networks, InfoWatch, McAfee, Fortinet, Crowdstrike, Trend Micro,

[3] O'zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi PF-60-son «2022 - 2026 yillarga mo'ljallangan Yangi O'zbekistonning Taraqqiyot strategiyasi to'g'risida» gi Farmoni

SababaSecurity, CyberGamp, Gen Digital, IBM, CyberArk и Cisco проводятся научно-практические и инженерно-исследовательские работы, направленные на оптимизацию правил сетевых пакетов и разработку новых типов аппаратно-программных межсетевых экранов.

В Республике Узбекистан научными коллективами под руководством Т.Ф.Бекмуратова, С.К.Ганиева, М.М.Каримова, Р.Х.Хамдамова, К.А. Ташева, Н.Б. Насруллаева, З.Т.Худойкулова, О.М.Алланова проводятся научные исследования по выявлению и предотвращению вторжений в информационно-коммуникационные системы, управлению моделями информационной безопасности, повышению эффективности методов и средств ограничения доступа в компьютерных сетях.

В то же время системы обнаружения аномалий и противоправных действий в сетевом трафике, модели предотвращения вредоносного трафика на DNS-серверах, фильтрация трафика на основе DSCP для предотвращения сетевых атак и методы реализации фильтрации трафика в сетях SDN, а также алгоритмы оптимизации правил фильтрации трафика недостаточно изучены в информационно-коммуникационных системах.

Связь диссертационного исследования с планами научно-исследовательских работ учреждения, в котором выполнена диссертация. Диссертационное исследование выполнено в рамках проектов Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий 598661-EPP-12018-1-RO-EPPKA2-CBHE-JP "Developing Services for Individuals with Disabilities–DECIDE" (2019-2022 годы), 598092-EPP-1-2018-1-BG-EPPKA2-CBHE-SP "Modernisation of Higher Education in Central Asia through New – HiEdTec" (2019-2022 годы) и UNICEN "Accreditation, Assessment, and Improving Student Outcomes" (2021-2022 годы).

Целью исследования является совершенствование и разработка методов и средств фильтрации сетевого трафика, позволяющих повысить эффективность защиты информационно-коммуникационных систем.

Задачи исследования:

классификация методов измерения пропускной способности сетевого трафика и сравнительный анализ методов фильтрации сетевого трафика в информационно-коммуникационных системах;

разработка информационной модели обнаружения и идентификации аномальных явлений в сетевом трафике;

усовершенствование модели для предотвращения вредоносного трафика и защиты от сопутствующих атак на DNS-сервера;

усовершенствование метода фильтрации сетевого трафика на основе кодовой точки дифференциальных служб;

усовершенствование метода минимизации потерь сетевых пакетов и повышения качества их обслуживания;

разработка алгоритмов обнаружения рисков в правилах фильтрации пакетов в зависимости от поведения сетевого трафика;

разработка алгоритмов защиты веб-ресурсов от вредоносных ботов и подозрительных пакетов в сетевом трафике.

В качестве **объекта исследования** были принят поток данных информационно-коммуникационных систем в контексте сетевой безопасности.

В качестве **предмета исследования** были выбраны методы и алгоритмы фильтрации сетевого трафика в информационно-коммуникационных системах.

Методы исследования. В исследовании используются методы, базирующиеся на основных положениях теории вероятностей, методов защиты информации, математического моделирования, искусственного интеллекта, объектно-ориентированных языков программирования, а также на результатах экспериментальных исследований по определению их достоверности с использованием программного средства.

Научная новизна исследования заключается в следующем:

на основе оценки и мониторинга сетевого трафика разработана информационная модель для минимизации воздействия внешних угроз и выявления сетевых аномалий путем предоставления предупреждений об уязвимостях и сбоях сети;

на основе методов машинного обучения усовершенствована модель устранения вредоносного трафика для обнаружения и блокировки вредоносных запросов к DNS-серверам и защиты от других типов DNS-трафика, включая DDoS-атаки;

на основе кодовой точки дифференциальных служб усовершенствован метод фильтрации для устранения перегрузки DHCP-сервера за счет установки правила ограничения максимального количества DHCP-пакетов и снижения риска конфликтов IP-адресов в сети;

за счет добавления псевдозаголовка TCP усовершенствован метод нормализации потока сетевого трафика, маскировки обмена данными и управления задержкой передаваемых сетевых пакетов, а также повышения качества обслуживания сетевого трафика и минимизации потерь сетевых пакетов с помощью корреляции датчиков;

разработаны алгоритмы минимизации рисков информационной безопасности в соответствии с поведением сетевого трафика и повышения производительности фильтрации пакетов за счет использования нечеткой фильтрации и отражения высшего приоритета правил при приеме или отклонении сетевых пакетов;

на основе блоков обработки веб-запросов разработаны алгоритмы защиты веб-ресурсов от вредоносных ботов, проверки подлинности веб-страниц, защиты доменов от онлайн-угроз и ложных фишинговых атак, а также минимизации ложных сообщений в системе.

Практические результаты исследования заключаются в следующем:

в сетях SDN на основе оркестратора и модулей фильтрации пакетов усовершенствован метод мониторинга потоков трафика и предотвращения любого вредоносного или нежелательного контента, который может попасть в сеть;

оптимизированы алгоритмы фильтрации для сокращения времени

обработки сетевых пакетных правил, переполнения и избыточности пакетов, а также минимизации атак IP-Spoofing в сетевом трафике по мере увеличения количества узлов на межсетевом экране;

разработан алгоритм проверки подлинности веб-страницы, защиты доменов от ложных фишинговых атак, онлайн-угроз и атак нулевого дня с использованием функций гиперссылок;

разработано программное средство блокировки запросов DDoS-атак, реализации открытого VPN-сервиса, мониторинга журналов URL-фильтрации, фильтрации информации по местоположению, реализации IP-таблиц и минимизации попадания вредоносных кодов в систему на основе многофакторного анализа трафика.

Достоверность результатов исследования. Соответствие подхода и методов целям исследования объясняется тем, что данные получены из официальных источников, в том числе статистических данных ГУП «Центр кибербезопасности», а соответствующие выводы и предложения были внедрены в практику со стороны ведущих организаций.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования состоит из разработанной информационной модели обнаружения и идентификации аномальных явлений, модели обнаружения и предотвращения вредоносных запросов в DNS-серверах, метода фильтрации сетевого трафика на основе кодовой точки дифференциальных служб, метода минимизации потерь сетевых пакетов и повышения качества их обслуживания, совершенствования и оптимизации алгоритмов сетевых пакетных правил в информационно-коммуникационных системах.

Практическая значимость результатов исследования заключается в минимизации рисков сетевых пакетов, защите веб-ресурсов от вредоносных ботов и подозрительного трафика, блокировке запросов DDoS-атак, реализации открытых VPN-сервисов, мониторинге журналов URL-фильтрации, фильтрации информации по местоположению и минимизации проникновения вредоносного кода в систему с помощью программного средства, разработанного на основе предложенных моделей, методов и алгоритмов.

Внедрение результатов исследования. На основе полученных научных результатов о методах и средствах фильтрации сетевого трафика в информационно-коммуникационных системах:

программное средство UzFirewall-next generation firewall, разработанное на основе архитектуры фильтрации веб-ресурсов в защите от веб-атак, было внедрено в практическую деятельность информационной системы хокимията Мирзо-Улугбекского района города Ташкента (Министерство цифровых технологий, Справка № 33-8/916 от февраля 2024 года). В результате научных исследований программное средство UzFirewall-next generation firewall по сравнению с Kerio Control 8.3.0 при скорости передачи данных 1 Гбит/с и в среднем размере пакета 12000 бит позволяет работать в 2,7 раз быстрее, то есть время обработки пакетов в Kerio Control 8.3.0 составляет 0,000005 секунды и

в UzFirewall-next generation firewall составляет 0,000002 секунды;

программное средство UzFirewall-next generation firewall, разработанное на основе метода предотвращения перегрузки DHCP-сервера путем установки правила для ограничения максимального количества пакетов DHCP, а также снижения риска конфликтов IP-адресов и на основе алгоритмов проверки подлинности веб-страницы, а также онлайн-угроз и атак нулевого дня с использованием функций гиперссылок, было внедрено в практическую деятельность Министерства культуры Республики Узбекистан (Министерство цифровых технологий, Справка № 33-8/916 от февраля 2024 года). В результате научных исследований программное средство UzFirewall-next generation firewall позволило обнаружить и предотвратить возможные сетевые атаки в информационной системе министерства с точностью 96%;

программное средство UzFirewall-next generation firewall, разработанное на основе архитектуры и алгоритмов для изменения действия правил в зависимости от поведения сетевого трафика, обеспечения высокоуровневого обслуживания важных данных и повышения качества сетевого обслуживания, а также отражения высшего приоритета правил приема и отклонения сетевых пакетов, было внедрено в практическую деятельность корпоративной сети территориального отдела города Ташкента инспекции «Узкомназорат» при Министерстве цифровых технологий Республики Узбекистан (Министерство цифровых технологий, Справка № 33-8/916 от февраля 2024 года). В результате научных исследований программное средство UzFirewall-next generation firewall показало результаты работы в 3 раза эффективнее от исходного состояния максимальной пропускной способности, при котором относительная масштабируемость составляла 300%, а также было установлено, что производительность при максимальной нагрузке по сравнению с производительностью при нормальной нагрузке в этом средстве увеличилась на 250%, т.е. в 2,5 раза;

программное средство UzFirewall-next generation firewall, разработанное на основе метода оптимизации потока сетевого трафика путем добавления псевдозаголовка TCP, уменьшения количества сбоев в сети, маскировки обмена данными путем изменения номера порта псевдозаголовка TCP и управления задержкой передаваемых сетевых пакетов, было внедрено в практическую деятельность сети, связи и телефонии в Самаркандском городском узле телекоммуникации АК "Узбектелеком" (Министерство цифровых технологий, Справка № 33-8/916 от февраля 2024 года). В результате научных исследований программное средство UzFirewall-next generation firewall позволило эффективно блокировать подозрительные пакеты в сетевом трафике на 95%. Применение данного программного средства позволило фильтровать информацию в сетевой системе и выявлять в ней подозрительные пакеты с высокой точностью, также повысить эффективность обеспечения информационной безопасности в информационной сети организации;

программное средство UzFirewall-next generation firewall, разработанное на основе метода реализации фильтрации трафика в сетях SDN и алгоритмов

обнаружения вредоносного трафика на рабочих станциях, было внедрено в практическую деятельность корпоративной сети Агентства по оценке знаний и квалификаций при Министерстве высшего образования, науки и инноваций Республики Узбекистан (Министерство высшего образования, науки и инноваций Республики Узбекистан, Справка №3/22-21/02-02 от февраля 2024 года). В результате исследования среднее время реакции программного средства UzFirewall-next generation firewall на сетевые атаки в течение 2 часов составило 2,6 минуты. Как видно из представленных выше результатов, данное программное средство позволило быстрее реагировать на атаки;

программное средство UzFirewall-next generation firewall, разработанное в результате совершенствования и оптимизации алгоритмов правил фильтрации пакетов, было внедрено в практическую деятельность корпоративной сети ООО «UZINFOCOM, единый интегратор по созданию и поддержке государственных информационных систем» (Министерство цифровых технологий, Справка № 33-8/916 от февраля 2024 года). В результате исследования программное средство UzFirewall-next generation firewall позволило за 1 час проанализировать 9456 пакетов из 11230 в системе и эффективность фильтрации пакетов составила 84%;

программное средство UzFirewall-next generation firewall, разработанное на основе предложенных методов, алгоритмов и архитектур, было внедрено в практическую деятельность корпоративной сети ООО «ИТ Парк инноваций в кибернетике» (ГУП «Центр кибербезопасности», Справка №03-18-01/410 от февраля 2024 года). В ходе тестирования данное средство обнаружило в общем 9764 события за 1 час, из них 546 атак и 22 ложных предупреждений. При этом можно увидеть, что доля ложных предупреждений средств составила 4%. Также, полученные показатели позволяют определить, насколько быстро система реагирует и блокирует атаки, оценить время реакции с течением времени, выявлять тенденции появления атак и изменения времени отклика межсетевых экранов, а также совершенствовать стратегии и процессы сетевой безопасности;

программное средство UzFirewall-next generation firewall, разработанное на основе метода фильтрации сетевого трафика и алгоритмов минимизации времени обработки правил сетевых пакетов, было внедрено в практическую деятельность корпоративной сети в «Центр развития информационно-коммуникационных технологий» при Государственном комитете автомобильных дорог Республики Узбекистан («Центр развития информационно-коммуникационных технологий» при Государственном комитете автомобильных дорог Республики Узбекистан, Справка №24/32 от апреля 2024 года). В результате исследования программное средство UzFirewall-next generation firewall, позволило обнаружить около 92% всех текущих сетевых аномалий по критерию чувствительности и около 84% всех событий, классифицированных как сетевые аномалии по критерию точности;

программное средство UzFirewall-next generation firewall, разработанное на основе алгоритмов защиты веб-ресурсов от вредоносных ботов и подозрительных пакетов, было внедрено в практическую деятельность

корпоративной сети Центра развития систем «Безопасный город» Министерства внутренних дел Республики Узбекистан (Центр развития систем «Безопасный город» Министерства внутренних дел Республики Узбекистан, Справка №03/419 от апреля 2024 года). В ходе тестирования программного средства UzFirewall-next generation firewall, при оценке характеристик сетевых пакетов на основе функции распределения Гаусса было отмечено, что вероятность принадлежности сетевых пакетов к обычному трафику составляет примерно 0,7%, а вероятность принадлежности к атакующему трафику 0,2%. Данный показатель позволил количественно оценить эффективность методов классификации сетевого трафика и определить их производительность.

Апробация результатов исследования. Результаты данного исследования обсуждались на 9 международных и 10 республиканских научно-практических конференциях.

Опубликованность результатов исследования. Всего по теме диссертации опубликовано 37 научных работ, в том числе 15 статей в научных изданиях, которые рекомендуются ВАК Республики Узбекистан к публикации основных научных результатов диссертаций, из них 10 опубликованы в зарубежных и 5 в республиканских журналах, получено 3 свидетельства о регистрации программных средств, созданных для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, пяти глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 184 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении приводятся актуальность и востребованность темы диссертации, обосновано соответствие исследования приоритетными направлениями развития науки и технологий Республики Узбекистан, определены цель и задачи, объект и предмет исследования, степень изученности проблемы, обоснована достоверность полученных результатов, раскрыто теоретико-практическое значение исследования. Приведена информация о внедрении в практику результатов исследования, представлены сведения по опубликованным работам, структуре и объему диссертации.

Первая глава диссертации **«Анализ методов защиты сетевого трафика в информационно-коммуникационных системах»** посвящена методам обеспечения безопасности сетевого трафика, анализу методов измерения пропускной способности и проблем классификации сетевого трафика, а также существующих методов классификации и фильтрации сетевого трафика в информационно-коммуникационных системах.

Формирование систем цифровой экономики в Республике, организация усиленного взаимодействия между органами государственного управления и населения осуществляется с использованием сети. Эффективное использование сети обеспечивает формирование информированного демократического общества. В таком обществе возрастет скорость обмена

информацией, сбор, хранение, обработка и использование информации будет иметь быстрый результат. По результатам анализа количество DDoS-атак продолжает расти всём мире и по данным Cisco, к концу 2023 года этот рост может привести к увеличению количества атак более чем вдвое по сравнению с 2018 годом. На рисунке 1 представлены среднегодовые темпы роста DDoS-атак с 2018 по 2023 годы.

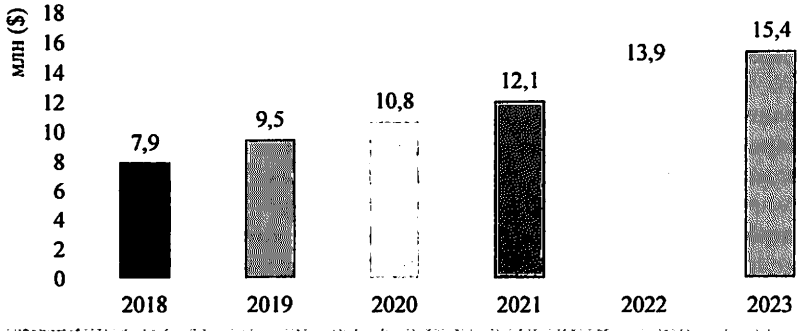


Рисунок 1. Среднегодовые темпы роста DDoS-атак в 2018-2023 гг.

Угрозы, возникающие в результате атак на распределенные информационно-коммуникационные системы, требуют эффективных методов обнаружения и реагирования. Наибольшую проблему вызывают атаки, с аномальным поведением в свойстве набора атрибутов выбранного сетевого трафика.

Одним из направлений развития систем фильтрации трафика является классификация сетевого трафика, позволяющая контролировать качество обслуживания и эффективно управлять пропускной способностью каналов. С увеличением количества подходов возникла необходимость их классификации. Методы классификации трафика представлены на рисунке 2.

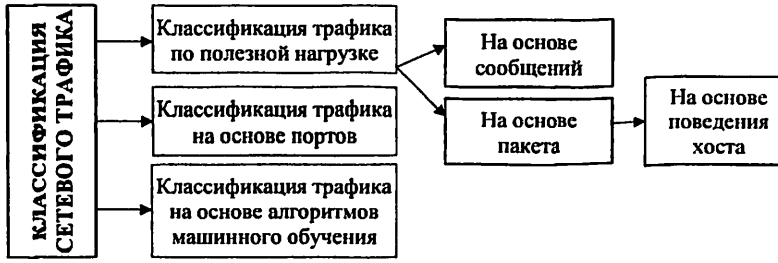


Рисунок 2. Методы классификации сетевого трафика

В этом характеристики аномального поведения и полезная нагрузка хостов и портов определяются на основе анализа методов классификации сетевого трафика. Это позволяет создать более совершенную систему контроля качества обслуживания и фильтрации трафика в сети.

Во второй главе диссертации **«Модели обнаружения вредоносного трафика в информационно-коммуникационных системах»**

проанализированы виды и методы обнаружения вредоносного трафика в сети. В результате анализа этапов обнаружения сетевых аномалий и незаконных действий в сетевом трафике был разработан алгоритм обнаружения аномалий и незаконных действий в сетевом трафике. На основе управления и анализа сетевых состояний предложена информационная модель идентификации сетевого трафика. Была усовершенствована модель предотвращения вредоносного трафика на DNS-серверах с использованием обучения классификаторов сетевого трафика и методов машинного обучения.

Обнаружение аномалий в сетевом трафике, как правило, предполагает необходимость тем или иным образом охарактеризовать нормальные данные, создать модель и рассматривать любые отклонения от нее как аномальные. При этом встречаются следующие серьезные трудности:

– сложность определения нормальных данных, неопределенность границы между нормальными и аномальными данными;

– маскировка действий злоумышленника для придания данным нормального вида;

– развитие систем генерации данных приводит к изменению понятия нормальности с течением времени;

– отсутствие нормальных и аномальных данных в обучающих классификаторах.

Чтобы минимизировать вышеперечисленные недостатки на рисунке 3 приведена блок-схема алгоритма обнаружения аномалий и незаконных действий в сетевом трафике.

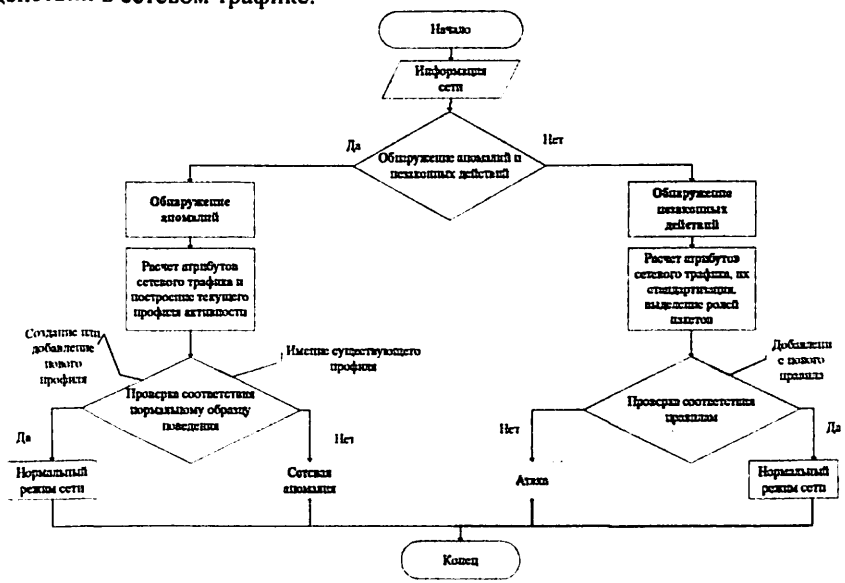


Рисунок 3. Блок-схема алгоритма обнаружения аномалий и незаконных действий в сетевом трафике

Более того, считается целесообразным создание информационной модели как объекта управления сети при идентификации сетевого трафика. На рисунке 4 предложена информационная модель для идентификации сетевого трафика.

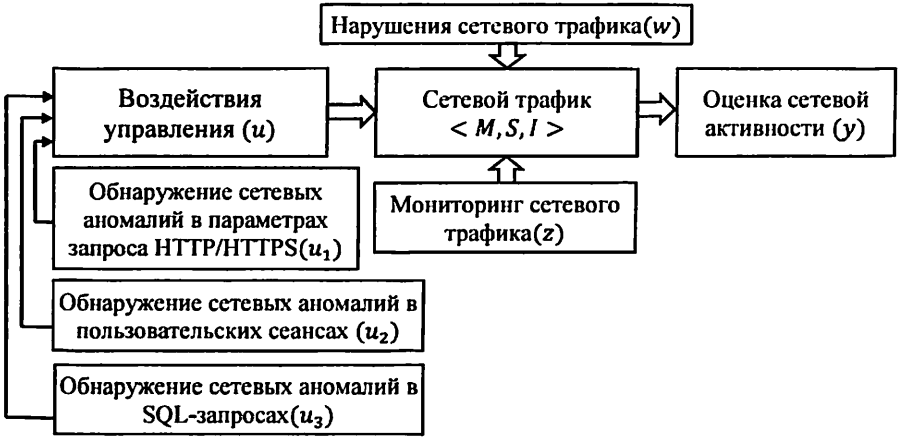


Рисунок 4. Информационная модель идентификации сетевого трафика

Информационную модель идентификации сетевого трафика можно выразить следующим образом:

$$y = f(M, S, I, u, z, w), \quad (1)$$

здесь, M —набор данных сетевого трафика; S —набор сетевых политик; I — набор данных внешних воздействий; u —воздействия управления; z — мониторинг сетевого трафика; w —нарушения сетевого трафика; y — оценка сетевой активности. Ниже приведено математическое представление функции $y = f(M, S, I, u, z, w)$:

$$y = f(M, S, I, u, z, w) = [f_1(M, S, I, u, z, w), f_2(M, S, I, u, z, w), f_3(M, S, I, u, z, w), \ldots, f_r(M, S, I, u, z, w)] \quad (2)$$

Каждая подфункция $y = f_i(M, S, I, u, z, w)$ выполняется следующим образом:

$$y = f_1(M, S, I, u, z, w) = g_1(M) + h_1(S) - \Sigma(I) + \Sigma(u) - \Sigma(z) - \Sigma(w)$$

$$y = f_2(M, S, I, u, z, w) = \alpha_2 g_2(M) + \beta_2 h_2(S) + \gamma_2 \Sigma(I) - \delta_2 \Sigma(u) - \varepsilon_2 \Sigma(z) + \varphi_2 \Sigma(w)$$

$$y = f_3(M, S, I, u, z, w) = (g_3(M) + h_3(S))\text{^}2 + \alpha_3 \Sigma(I) + \beta_3 \Sigma(u) - \gamma_3 \Sigma(z) + \delta_3 \Sigma(w)$$

$$y = f_r(M, S, I, u, z, w) = \alpha_r g_r(M) - \beta_r h_r(S) + \gamma_r \Sigma(I) - \delta_r \Sigma(u) + \varepsilon_r \Sigma(z) - \varphi_r \Sigma(w) \quad (3)$$

В этих выражениях:

– $g_i(M)$ и $h_i(S)$ – функции, которые выполняют операции с набором данных сетевого трафика M и набором сетевых политик S соответственно;

– $\Sigma(I), \Sigma(u), \Sigma(z)$ и $\Sigma(w)$ выражает сумму элементов векторов I, u, z и w соответственно;

– $\alpha_i, \beta_i, \gamma_i, \delta_i, \varepsilon_i$ и φ_i –измерительные коэффициенты различных компонентов;

– математические операции $(+, -, \Sigma, \hat{}2)$ включают арифметические операции, статистические функции и другие связанные математические операции, основанные на требованиях системы обнаружения аномалий.

В целом, предложенная информационная модель позволяет выявлять возможные сетевые аномалии и уязвимости сетевого трафика и снижать риски информационной безопасности.

Таким образом, на основе информационной модели идентификации сетевого трафика, модель устранения вредоносного трафика на DNS-серверах может быть реализована в следующие два этапа.

1-этап: на рисунке 5 предложена модель предотвращения вредоносного трафика на DNS-серверах при отправке запроса от клиента на сервер. Запрос от клиента к DNS-серверу сначала проходит через раздел фильтрации белого списка домена. Если в данной части название запроса классифицируется как безвредное, пакет направляется принимающей части. И наоборот, если запрос не соответствует белому списку, пакет пройдет через фильтрующую часть черного списка домена.

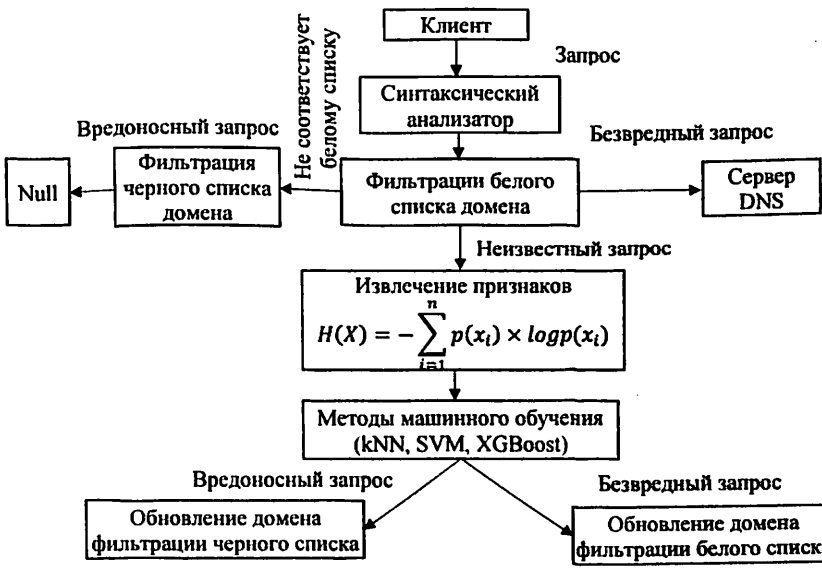


Рисунок 5. Модель предотвращения вредоносного трафика на DNS-серверах: запрос клиент-сервер

В этой части, когда запрос классифицируется как вредоносный, пакет возвращается на NULL-устройство. И наоборот, если запрос не соответствует черному списку домена, пакет направляется получателю. Затем часть извлечения признаков преобразует *qname* в векторы признаков и часть классификатора классифицирует запрос. Если результат классификации показывает, что пакет безвреден, запрос добавляется в белый список домена. И наоборот, если результат является вредоносным, запрос добавляется в черный список домена, блокируются DNS-запросы, содержащие такой запрос, без обработки методами машинного обучения.

2-этап: на рисунке 6 предложена модель предотвращения вредоносного трафика на DNS-серверах при отправке запроса с сервера клиенту.

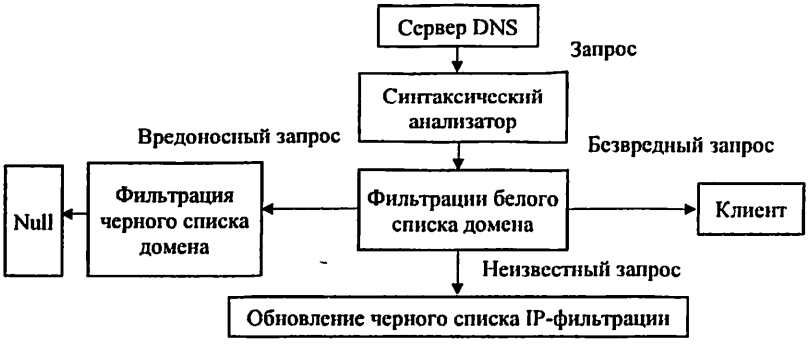


Рисунок 6. Модель предотвращения вредоносного трафика на DNS-серверах: запрос сервер-клиент

При отправке запроса с сервера клиенту ответ DNS от DNS-сервера сначала проходит через фильтрацию белого списка домена. Если в данной части запрос классифицируется как безвредный, пакет направляется принимающей части. И наоборот, если запрос не соответствует белому списку, пакет направляется в фильтрующую часть черного списка домена. Если в этой части запрос классифицируется как вредоносный, пакет удаляется системой и проверяется в ответном сообщении. В таблице 1 представлены результаты тестирования по предотвращению вредоносного трафика на DNS-серверах методами машинного обучения.

Таблица 1

Результаты тестирования по предотвращению вредоносного трафика на DNS-серверах методами машинного обучения

Набор данных		Методы машинного обучения	Обучение (80%)	Тестирование (20%)
Число	33925 строк	kNN	100	91.97
Класс	DrDos_DNS	SVM	100	90.94
Свойства	15	XGBoost	100	91.92

Здесь обучение набора данных проводилось с использованием языка программирования Python, а результаты тестирования были представлены с помощью компилятора Jupyter. Данная совершенная модель предотвращения

вредоносного трафика на DNS-серверах позволяет обнаруживать вредоносные запросы клиентов к DNS-серверу на основе методов машинного обучения и защищать от других типов атак, связанных с DNS-трафиком, включая фишинг, DDoS.

В третьей главе диссертации **«Усовершенствованные методы фильтрации сетевого трафика в информационно-коммуникационных системах»** усовершенствован метод фильтрация сетевого трафика на основе кодовой точки дифференциальных служб, позволяющий минимизировать некоторые известные сетевые атаки, реализуемые злоумышленниками, такие как DHCP-запросы и риска конфликтов IP-адресов, а также предложен метод повышения качества обслуживания и минимизации потерь сетевых пакетов за счет добавления псевдозаголовка TCP. Усовершенствованы методы снижения риска сбоев серверов и рабочих станций, мониторинга потоков трафика, упрощения управления правилами фильтрации пакетов, а также предотвращения любого вредоносного или нежелательного контента, который может проникнуть в сеть.

Протокол DHCP позволяет автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. На рисунке 7 предложена схема фильтрации пакетов DHCP на основе DSCP, начиная с процесса регистрации, который должен выполнить каждый клиент WLAN, подключающийся к сети.

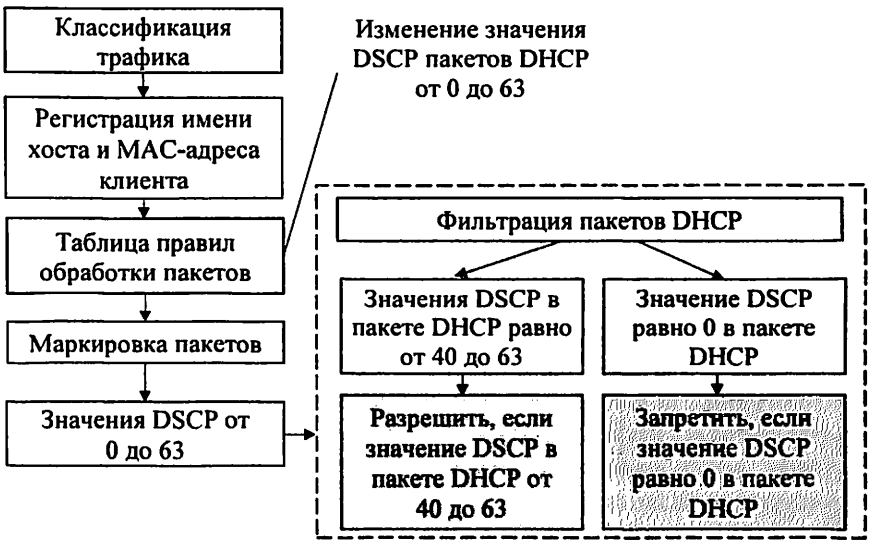


Рисунок 7. Схема фильтрации пакетов DHCP на основе DSCP

В данном случае данный протокол работает по модели клиент-сервер и позволяет пользователям подключаться через локальную сеть или сеть Интернет. Протокол DHCP автоматически настраивает необходимый IP-адрес

для каждого клиента. Более того, значение DSCP пакета DHCP, отправленного от незарегистрированного клиента, изменяется на 0. На следующем этапе функция фильтрации фильтрует каждый пакет DHCP напрямую, если DSCP пакета DHCP имеет значение от 40 до 63, разрешается направить пакет на следующий этап. В противном случае пакет DHCP будет удален.

Для минимизации потерь сетевых пакетов и повышения качества их обслуживания используется псевдо-заголовок TCP. После прохождении фильтрации передаваемый пакет восстанавливается в исходную форму путем удаления псевдо-заголовок TCP. На рисунке 8 предложена схема фильтрации трафика путем добавления псевдо-заголовок TCP.

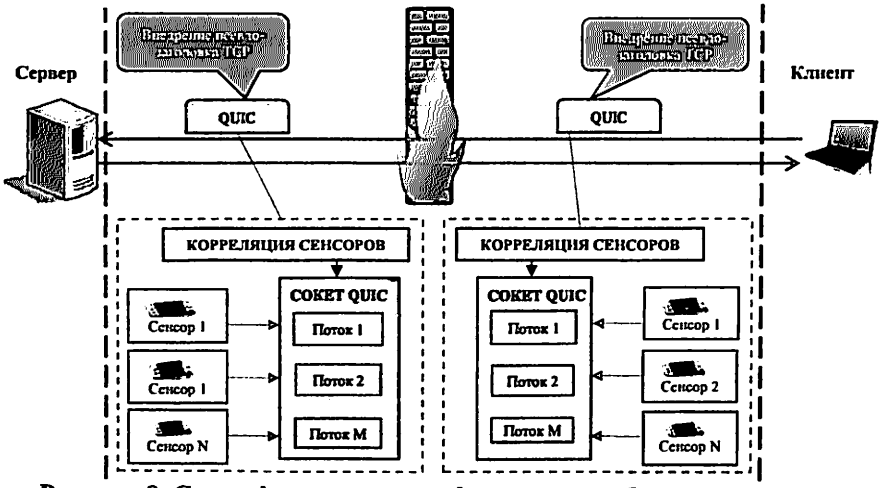


Рисунок 8. Схема фильтрации трафика путем добавления псевдо-заголовка TCP

Псевдо-заголовок TCP позволяет маскировать обмен данными путем изменения номера порта, управлять задержкой передаваемых сетевых пакетов, а также менять порты для протоколов, которые случайным образом выбирают порты из широкого диапазона. При передаче пакетов с помощью протокола QUIC каждый поток рассматривают сенсора как отдельный объект. Поскольку сенсоры выдают несколько показаний в секунду, рекомендуется использовать не только разные потоки для каждого сенсора, но и разные потоки для каждого объекта. Когда все пакеты, отправленные в поток, подтверждены, поток можно повторно использовать для нового объекта. И наоборот, если поток блокируется из-за потери пакетов и данные устарели, отправитель отправляет получателю кадр с просьбой удалить все существующие данные, находящиеся не в порядке, из этого потока и восстановить поток. Несколько сенсоров записывают данные в сокет QUIC и предоставляют матрицу корреляции между сенсорами. Таким образом, предложенный метод позволяет маскировать обмен данными путем изменения номера порта псевдозаголовка TCP,

контролировать задержку передаваемых сетевых пакетов.

Программно-определяемая сеть (SDN) обеспечивает интеллектуальное и централизованное управление сетью. Это позволяет операторам последовательно и комплексно управлять всей сетью, независимо от базовой технологии, используемой в сети. Таким образом, усовершенствован метод реализации фильтрации трафика в сетях SDN позволяющий повысить безопасность сетевого трафика. На рисунке 9 приведена схема работы модулей фильтрации пакетов.

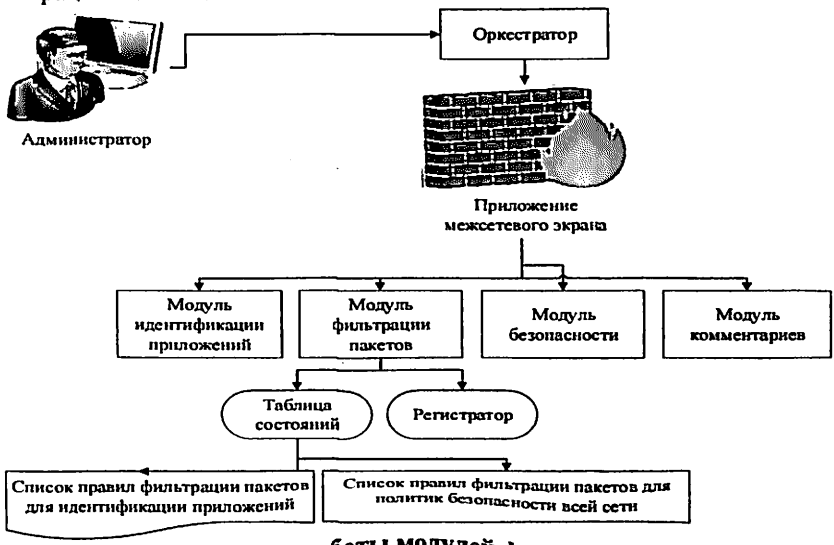


Рисунок 9. Схема работы модулей фильтрации пакетов

В предложенной схеме функция межсетевого экрана реализована с помощью четырех взаимодействующих модулей: модуля идентификации приложений, модуля фильтрации пакетов, модулей безопасности и комментариев. В результате реализации модулей предложенной схемы видно, что метод реализации фильтрации трафика в сетях SDN позволяет контролировать потоки трафика, упрощать управление безопасностью и предотвратить любой нежелательный контент.

Глава четвертая диссертации **«Алгоритмы обнаружения и предотвращения подозрительных сетевых пакетов в информационно-коммуникационных системах»** посвящена разработке алгоритмов изменения действия правил в зависимости от поведения трафика, минимизации рисков в сетевых пакетах, а также отражения наивысшего приоритета правил при приеме или отклонении сетевых пакетов. Оптимизированы алгоритмы упорядочивания правил фильтрации для сокращения времени обработки сетевых пакетных правил, минимизации переполнения пакетов и атак IP-Spoofing в сетевом трафике по мере увеличения количества узлов на межсетевом экране. Разработан алгоритм

защиты веб-ресурсов от вредоносных ботов и подозрительного трафика, а также предотвращения от существующих и новых веб-атак на основе многофакторного анализа трафика. Предложен алгоритм проверки подлинности веб-страницы и защиты домена от ложных фишинговых атак, онлайн-угроз и атак нулевого дня с использованием функций гиперссылок.

Нечеткая сеть Петри представляет собой комбинацию нечеткой логики и сетей Петри. Нечеткая сеть Петри представляет собой средство выражения неопределенных знаний о состоянии системы и обладает способностью описывать неопределенные события и правила действий. Нечеткая модель сети Петри описывается как набор $N_f(P,T,D,I,\alpha,\beta)$. Нечеткая сеть Петри используется в качестве графического метода для описания нечетко-логического управления пакетным трафиком через межсетевой экран и описывается следующим выражением:

$$f: U \subset \bigcup_{i=1}^{n} (R_i \cap V), \qquad (4)$$

здесь, $U = U_1 \times U_2$–входящее пространство; V –выходящее пространство; R –уровень риска.

Первый уровень: нечеткая фильтрация. Данный уровень основан на перехвате и классификации всех входящих пакетов на основе данных, связанной с каждым пакетом, таких как IP-адрес, время пакета и тип протокола, имитация и отслеживание пакетов. На рисунке 10 "а" предложена блок-схема алгоритма правил фильтрации пакетов.

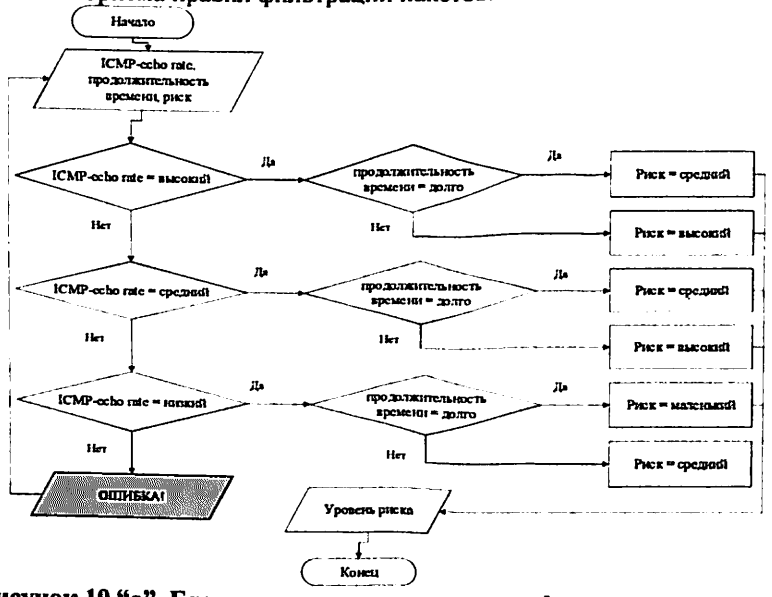


Рисунок 10 "а". Блок-схема алгоритма правил фильтрации пакетов (первый уровень: нечеткая фильтрация)

Пакет представлен токеном через нечеткую сеть Петри, и нечеткая сеть Петри отвечает за обработку и перемещение пакета из одного места в другое.

Второй уровень: нечеткая фильтрация. Обычно с каждым межсетевым экраном связано два набора пакетов: набор пакетов, принятых межсетевым экраном, и набор пакетов, отклоненных межсетевым экраном. На рисунке 10 "б" предложена блок-схема алгоритма правила фильтрации пакетов. В данном случае используется нечеткая логика с двумя входами и одним выходом.

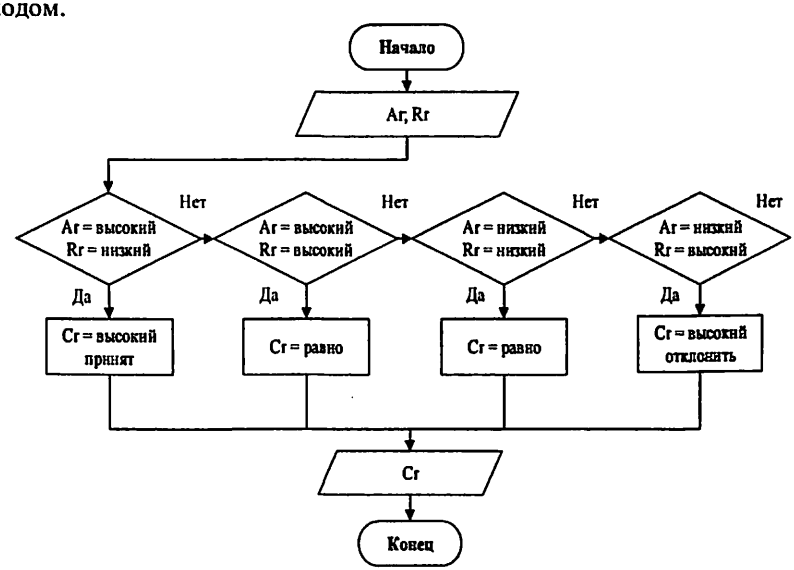


Рисунок 10 "б". Блок-схема алгоритма правила фильтрации пакетов (второй уровень: нечеткая фильтрация)

Две нечеткие переменные, "низкий" и "высокий", используются для описания скорости принятия A_r и скорости отклонения сетевых пакетов R_r. Результатом нечеткой логики является рассчитанная величина C_r, которая описывает скорости отклонения и принятия в трафике и характеризуется тремя нечеткими переменными, включая высокую скорость отклонения, равную и высокую скорость принятия.

Оптимизация алгоритмов правил фильтрации пакетов. Ниже проведены операции по оптимизации алгоритмов правил фильтрации пакетов по критерию избыточности пакетов. Каждое избыточное правило увеличивает сложность и стоимость анализа трафика, поэтому уменьшение их количества обеспечить систему более стабильной.

Предположим:

Пусть $Min \sum_{i=1}^{n} D_i \times x_i$ – будет целевой функцией.

Здесь, $D_i - i$ степень избыточности правил; $x_i - i$ переменные, определяющие, применения (1) или отклонения (0); n – количество правил фильтрации пакетов.

Минимизация избыточности правил фильтрации пакетов определяется на основе следующих границ:

1. $\sum_{i=1}^{n} a_{ij} \times x_i \geq b_j$ — ограничения безопасности;
2. $\sum_{i=1}^{n} r_{ij} \times x_i \geq R_j$ — ограничения ресурсов.

Здесь, a_{ij} —элемент матрицы, влияющий на ограничение безопасности правила j; b_j —необходимое минимальное значение ограничения безопасности правила j; r_{ij} —элемент матрицы правила i, влияющий на ресурс j; R_j —максимальное значение, выделенное для ресурса j. В результате оптимизации алгоритмов правил фильтрации трафика по мере увеличения количества узлов в межсетевом экране удается сократить время обработки сетевых пакетных правил, минимизировать переполнение и избыточность пакетов, а также атаки IP-Spoofing в сети. В таблице 2 представлены результаты оптимизации по уровням критерия обнаружения избыточности в правилах фильтрации пакетов.

Таблица 2

Результаты оптимизации по уровням критерия обнаружения избыточности в правилах фильтрации пакетов

№	Наименование алгоритма	Результаты оптимизации $Min \sum_{i=1}^{n} D_i \times x_i$
1.	Сжатия правил	5.4%
2.	Распределение правил	4.7%
3.	Генерация метаправил	7.1%
4.	Генерация непротиворечивых правил	5.3%

По мере увеличения числа пользователей Интернета возрастает значение фильтрации веб-трафика. Фильтрация веб-трафика - это тип обратного прокси-сервера, который защищает веб-сервер от воздействия клиента путем обнаружения подозрительного трафика. На рисунке 11 представлена блок-схема алгоритма фильтрации веб-ресурсов при защите от веб-атак. Более того, при идентификации подозрительных пакетов используется набор данных, который включает IP-адрес источника и назначения сетевых пакетов, порт, протокол, размер пакета и метки класса для каждого пакета, указывающие, является ли он подозрительным или нет. Этот набор следует описать следующим образом:

Признаки пакета. Каждый сетевой пакет характеризуется рядом признаков:

$$X = \{x_1, x_2, \dots, x_n\}, \quad (5)$$

здесь,

x_i —описывает уникальный признак пакета, например, IP-адрес, порт, протокол и т.д.

Метка класса. Если $y = 1$, пакет подозрительный, если y=0, пакет

нормальный, т.е.

$$(x) = \begin{cases} y = 1, & \text{пакет подозрительный} \\ y = 0, & \text{пакет нормальный} \end{cases} \quad (6)$$

Для определения доли подозрительных пакетов используется метод логистической регрессии на основе признаков пакета и меток класса, т.е.

$$LR_{\upsilon}(X) = \frac{1}{1 + e^{-\upsilon X}}, \quad (7)$$

здесь, υ —параметры вектора.

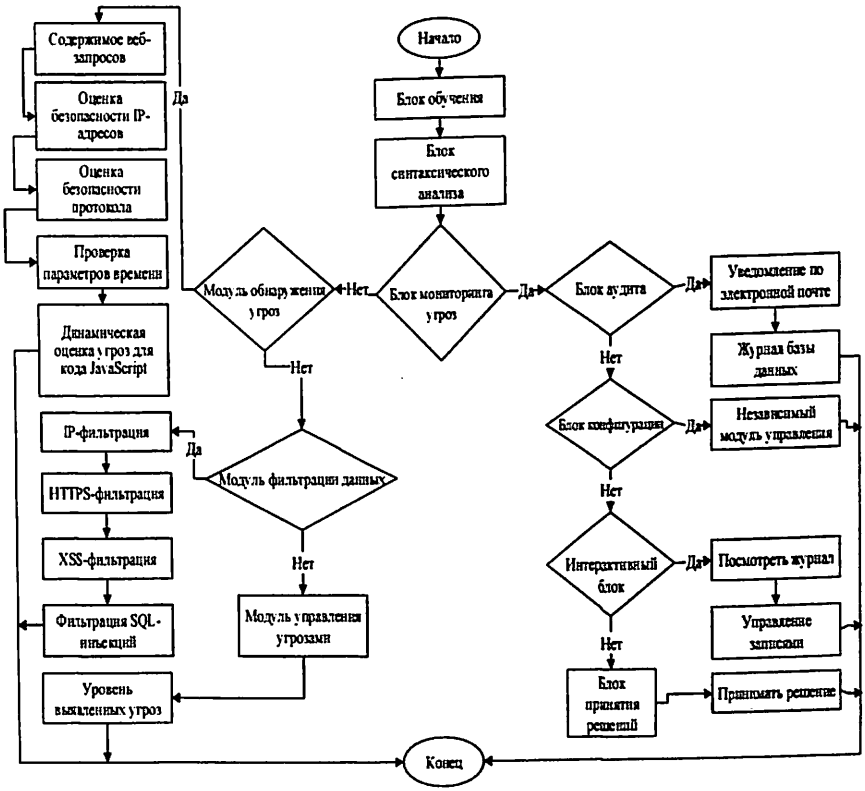


Рисунок 11. Блок-схема алгоритма фильтрации веб-ресурсов при защите от веб-атак

Данный алгоритм проверит веб-ссылку на безвредность, система предупреждает пользователя, если сайт является фишинговым система предупредит пользователя, если сайт безвреден, система обновляет домен из белого списка.

В пятой главе диссертации **«Оценка эффективности программного средства фильтрации трафика и результаты внедрения на практике»** разработано программное средство UzFirewall-next generation firewall позволяющее идентифицировать, отделять и блокировать сетевые пакеты,

пропущенные стандартными средствами фильтрации, минимизировать ложные сообщения за счет оптимизации количества правил фильтрации пакетов, блокировать запросы от DDoS-атак и минимизировать проникновение вредоносного кода. Данное программное средство было внедрено на практике в информационных центрах промышленных предприятий Республики Узбекистан, по итогу были получены результаты по фильтрации сетевого трафика, оптимизации правил фильтрации, обнаружения сетевых аномалий, ложных срабатываний и минимизации сетевых угроз.

Для обеспечения полной защиты информационных ресурсов компании, необходимо использовать программные решения для их защиты. В связи с этим предлагаемое программное средство UzFirewall-next generation firewall показало свою эффективность как современное решение и достаточный уровень безопасности для его регулярного применения. Оценка эффективности межсетевых экранов, в частности, с UzFirewall-next generation firewall, зафиксирована в таблицах 3, 4 и 5.

Критерий положительной прогностической ценности – Positive Predictive Value (PPV). Данный критерий позволяет определить количество правильно классифицированных пакетов. В таблице 3 представлена оценка эффективности межсетевых экранов по критерию PPV.

Таблице 3

Оценка эффективности межсетевых экранов по критерию PPV

Средства	$PPV = \frac{\text{Количество правильно классифицированных пакетов}}{\text{Общее количество пакетов}} \times 100$	%
ZyWALL ATP200	$PPV = \frac{1630}{1700} \times 100$	95,8
ZoneAlarm Free Firewall 15.8.213.19411	$PPV = \frac{1627}{1700} \times 100$	95,7
UzFirewall-next generation firewall	$PPV = \frac{1669}{1700} \times 100$	98,1
TinyWall	$PPV = \frac{1586}{1700} \times 100$	93,2
PrivateFirewall 7.0.30.3	$PPV = \frac{1591}{1700} \times 100$	93,5

Критерий полноты (Recall). Критерий полноты позволяет измерить способность обнаруживать все вредоносные пакеты в трафике. В таблице 4 представлена оценка эффективности межсетевых экранов по критерию полноты.

Таблица 4

Оценка эффективности межсетевых экранов по критерию полноты

Средства	$\text{Recall} = \frac{\text{Количество правильно классифицированных вредоносных пакетов}}{\text{Общее количество вредоносных пакетов}} \times 100$	%
ZyWALL ATP200	$\text{Полнота} = \frac{673}{700}$	96,1
ZoneAlarm Free Firewall 15.8.213.19411	$\text{Полнота} = \frac{671}{700}$	95,8
UzFirewall-next generation firewall	$\text{Полнота} = \frac{686}{700}$	98,0
TinyWall	$\text{Полнота} = \frac{639}{700}$	91,2
PrivateFirewall 7.0.30.3	$\text{Полнота} = \frac{640}{700}$	91,4

Критерий измерения F1 (F1-Score). В таблице 5 представлена оценка эффективности межсетевых экранов по критерию измерения F1.

Таблица 5

Оценка эффективности межсетевых экранов по критерию измерения F1 (F1-Score)

Средства	$F1 = 2 \times \frac{\text{PPV} \times \text{Recall}}{\text{PPV} + \text{Recall}}$	%
ZyWALL ATP200	$F1 = 2 \times \frac{95{,}8 \times 96{,}1}{95{,}8 + 96{,}1}$	95,9
ZoneAlarm Free Firewall 15.8.213.19411	$F1 = 2 \times \frac{95{,}7 \times 95{,}8}{95{,}7 + 95{,}8}$	95,7
UzFirewall-next generation firewall	$F1 = 2 \times \frac{98{,}1 \times 98}{98{,}1 + 98}$	98,0
TinyWall	$F1 = 2 \times \frac{93{,}2 \times 91{,}2}{93{,}2 + 91{,}2}$	92,1
PrivateFirewall 7.0.30.3	$F1 = 2 \times \frac{93{,}5 \times 91{,}4}{93{,}5 + 91{,}4}$	92,4

На рисунке 11 представлена диаграмма оценки эффективности межсетевых экранов по критерию измерения F1.

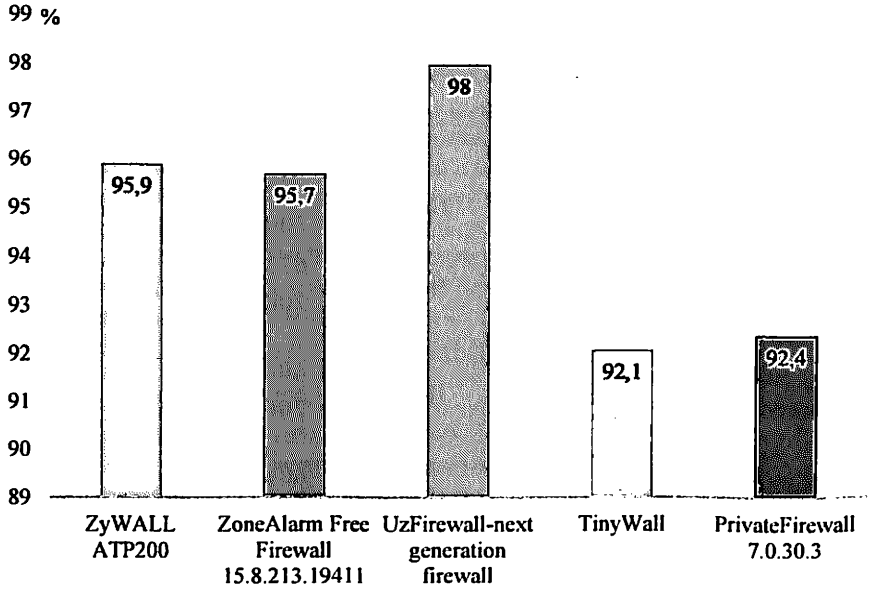


Рисунок 11. Оценки эффективности межсетевых экранов по критерию измерения F1

По результатам сравнительного анализа межсетевых экранов на основе вышеуказанных критериев оценки эффективность предлагаемого программного средства межсетевого экрана нового поколения UzFirewall-next generation firewall объясняется тем, что оно зафиксировало более высокие результаты, чем другие межсетевые экраны.

ЗАКЛЮЧЕНИЕ

По результатам диссертационной работы на тему «Методы и средства фильтрации сетевого трафика в информационно-коммуникационных системах» представлены следующие выводы:

1. Предложена информационная модель идентификации сетевого трафика. В результате удалось выявить и минимизировать влияние внешних угроз за счет выявления возможных уязвимостей в сетевом трафике и аномалий в параметрах HTTP/HTTPS и SQL-запросов.
2. На основе методов машинного обучения усовершенствована модель предотвращения вредоносного трафика на DNS-серверах. В результате это позволило анализировать, обнаруживать и блокировать входящие DNS-запросы от клиентов, обновлять черные и белые списки доменов и защищать от других типов атак, связанных с DNS-трафиком, включая фишинг, ботнеты, DDoS.
3. Предложен метод фильтрации сетевого трафика на основе кодовой

точки дифференциальных служб. В результате удалось минимизировать некоторые известные сетевые атаки, реализуемые злоумышленниками, такие как DHCP-запросы и риски конфликтов IP-адресов, предотвратить перегрузку DHCP-сервера, установив правило, ограничивающее максимальное количество пакетов DHCP.

4. Предложен метод минимизации потерь сетевых пакетов и повышения качества их обслуживания за счет добавления псевдо-заголовка TCP. В результате позволено нормализовать поток сетевого трафика, минимизировать сбои в сети, замаскировать обмен данными и управлять задержками передаваемых сетевых пакетов путем изменения номера порта псевдо-заголовка TCP.

5. Усовершенствован метод секретного портового стука в сетевом трафике. В результате были достигнуты последовательности стуков различной длины при одновременных попытках аутентификации для ускорения время обнаружения портов, а также снижения вероятности сбоев сервера и рабочей станции.

6. Усовершенствован метод фильтрации трафика в сетях SDN на основе оркестратора и модулей фильтрации пакетов. В результате было позволено произвести мониторинг потоков сетевого трафика, упростить управление правилами фильтрации пакетов и предотвратить любой вредоносный или нежелательной контент, который может проникнуть в сеть.

7. Разработаны двухуровневые алгоритмы нечеткой фильтрации пакетов. В результате были достигнуты изменение действия правил и минимизация рисков на сетевые пакеты в соответствии с поведением сетевого трафика, повышение производительности фильтрации пакетов за счет применения нечеткой фильтрации, а также отражение высшего приоритета правил при принятии или отклонении сетевых пакетов.

8. Оптимизированы алгоритмы упорядочивания правил фильтрации сетевого трафика. В результате с увеличением количества узлов на межсетевом экране были достигнуты сокращение времени обработки сетевых пакетных правил, минимизировано переполнение пакетов и атаки IP- Spoofing в сети, а также было зафиксировано, что оптимизация пакетов по уровням критерия избыточности в сумме составляет 5,62%.

9. На основе блоков обработки веб-запросов разработаны алгоритмы фильтрации веб-ресурсов и выявления подозрительных пакетов в сетевом трафике. В результате были достигнуты защиты веб-ресурсы от вредоносных ботов, проверка подлинность веб-страниц и защиты домены от онлайн-угроз и ложных фишинговых атак.

10. По результатам внедрения программного средства UzFirewall-next generation firewall в информационных центрах предприятий отрасли установлено, что скорость передачи данных в 2,7 раз быстрее, по сравнению с программным средством Kerio Control 8.3.0, точность предотвращения сетевых атак составила 96%, эффективность блокировки подозрительных пакетов составила 95%, эффективность фильтрация сетевых пакетов составила 84%, а также при оценке характеристик сетевых пакетов было отмечено, что

вероятность принадлежности сетевых пакетов нормальному трафику составляет примерно 0,7%, а вероятность принадлежности к атакующему трафику составляет 0,2%.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.02 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

GULOMOV SHERZOD RAJABOEVICH

METHODS AND TOOLS OF FILTERING NETWORK TRAFFIC IN INFORMATION-COMMUNICATION SYSTEMS

05.01.05 – Methods and systems of information protection. Information Security

ABSTRACT OF THE DISSERTATION OF DOCTOR OF TECHNICAL SCIENCES (DSc)

Tashkent-2024

The theme of doctor of technical sciences (DSc) was registered at the Supreme attestation commission at the Ministry of higher education, science and innovation of the Republic of Uzbekistan under number B2024.1.DSc/T770

The dissertation has been prepared at Tashkent University of Information Techologies named after Muhammad al-Khwarizmi.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website (www.tuit.uz) and on the website of «ZiyoNet» Information and educational portal (www.ziyonet.uz).

Scientific adviser:	**Karimov Madjit Malikovich** Doctor of technical sciences, professor
Official opponents:	**Rakhmatullaev Marat Alimovich** Doctor of technical sciences, professor
	Kerimov Kamil Fikratovich Doctor of technical sciences, docent
	Kuryazov Davlatyor Matyakubovich Doctor of physical and mathematical sciences
Leading organization:	**National University of Uzbekistan named after Mirzo Ulugbek**

The defense will take place "29th" June 2024 at 11:00 the meeting of Scientific council No. DSc.13/30.12.2019.T.07.02 at Tashkent University of Information Technologies (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi (is registered under No. 317). (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-65-44).

Abstract of dissertation sent out on "21th" June 2024 y.
(mailing report No. 13 on "21th" June 2024 y.).

B.Sh. Makhkamov
Chairman of the Scientific Council awarding scientific degrees, doctor of economic sciences, professor

M.S. Saitkamolov
Scientific secretary of Scientific Council awarding scientific degrees, doctor of economic sciences, docent

S.K. Ganiev
Chairman of the Academic seminar under the Scientific Council awarding scientific degrees, doctor of technical sciences, professor

INTRODUCTION (abstract of DSc dissertation)

The purpose of the research is to provide and manufacture a network traffic filtering method and production that allows to improve the protection of information and communication systems.

As the object of the research in the context of network security, the data flow of information and communication systems was taken.

The scientific novelty of the research is as follows:

based on assessment and monitoring of network traffic, an information model has been developed to minimize the impact of external threats and identify network anomalies by providing warnings about vulnerabilities and network failures;

based on machine learning methods, the malicious traffic elimination model has been improved to detect and block malicious requests to DNS servers and protect against other types of DNS traffic, including DDoS attacks;

based on the differential services code point, the filtering method has been improved to eliminate DHCP server overload by setting a rule to limit the maximum number of DHCP packets and reduce the risk of IP address conflicts on the network;

by adding a TCP pseudo-header, the method of normalizing the flow of network traffic has been improved, masking data exchange and managing the delay of transmitted network packets, as well as improving the quality of service of network traffic and minimizing the loss of network packets using sensor correlation;

algorithms have been developed to minimize information security risks in accordance with the behavior of network traffic and improve packet filtering performance through the use of fuzzy filtering and reflecting the highest priority of rules when accepting and rejecting network packets;

based on blocks for processing web requests, algorithms have been developed to protect web resources from malicious bots, verify the authenticity of web pages, protect domains from online threats and false phishing attacks, as well as minimize false messages in the system.

Implementation of research results. Based on the scientific results obtained on methods and tools of filtering network traffic in information-communication systems:

the UzFirewall-next generation firewall software tool was developed based on web resource filtering architecture to protect against web attacks, was implemented into the practical activity of application of the information system of the Mirzo Ulugbek district administration of Tashkent city (the reference of the Ministry of Digital Technologies No. 33-8/916 of February 2024). As a result of scientific research, the UzFirewall-next generation firewall software tool in comparison with Kerio Control 8.3.0, at a data transfer rate of 1 Gbit/s and an average packet size of 12000 bits, allows it to work 2.7 times faster, that is, the packet processing time in Kerio Control 8.3.0 is 0.000005 seconds and in UzFirewall-next generation firewall it is 0.000002 seconds;

the UzFirewall-next generation firewall software tool was developed on the basis a method to reduce the risk of IP address conflicts and to limit the maximum number of DHCP packets by setting a rule to limit the maximum number of DHCP

packets and to check the legitimacy of a web page using hyperlink functions and to protect domains from fake phishing attacks, online threats and zero attacks based on algorithms, was implemented into the practical activity of the Ministry of Culture of the Republic of Uzbekistan (the reference of the Ministry of Digital Technologies No. 33-8/916 of February 2024). As a result of the research, the UzFirewall-next generation firewall software tool allowed it possible to identify and prevent possible network attacks in the ministry's information system with 96% accuracy.

the UzFirewall-next generation firewall was developed on the basis of the architecture and algorithms to change the actions of rules according to traffic behavior, provide high-level service for important data and improve the quality of network service and reflect the highest priority of rules when receiving and discarding network packets software tool "Ozkomnazorat" inspection under the Ministry of Digital Technologies of the Republic of Uzbekistan was implemented into the practical activity of the corporate network of the regional department of the city of Tashkent (the reference of the Ministry of Digital Technologies No. 33-8/916 of February 2024). As a result of scientific research, the UzFirewall-next generation firewall software tool allowed to work 3 times more efficiently than its original maximum throughput state, in which the relative scalability was 300%, and the maximum load compared to the normal load performance in this tool was 250%, that is found to be 2.5 times higher;

the UzFirewall-next generation firewall software tool was developed based on the method of optimizing the flow of network traffic by adding a TCP pseudo-header, reducing the number of network crashes, masking data exchange by changing the TCP pseudo-header port number, and managing the delay of transmitted network packets and it was implemented into the practical activity of the communication and telephony network of Uzbektelecom JSC "Samarkand City Telecommunication Link" (the reference of the Ministry of Digital Technologies No. 33-8/916 of February 2024). As a result of scientific research, the UzFirewall-next generation firewall software tool enabled 95% efficiency in blocking suspicious packets in network traffic. The use of this software tool allowed to filter information in the organization's network system and identify suspicious packets in them with high accuracy, as well as to increase the efficiency of information security in the organization's information network;

the UzFirewall-next generation firewall software tool was developed on the basis of methods of filtering traffic in SDN networks and algorithms for detecting malicious parties in workstations tha it was implemented in the practical activity of the corporate network of the Agency for the Evaluation of Knowledge and Skills under the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan (the reference of the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan No. 3/22-21/02-02 of February 2024). As a result of the research, the average response time of UzFirewall-next generation firewall software tool to network attacks during 2 hours was 2.6 minutes. As can be seen from the results presented above, this software tool allowed it possible to respond to attacks faster;

the UzFirewall-next generation firewall software tool was developed as a result

of improving and optimizing the algorithms of packet filtering rules, that it was implemented into the practical activity of the corporate network of "UZINFOCOM Single Integrator for the Creation and Support of State Information Systems" LLC (the reference of the Ministry of Digital Technologies No. 33-8/916 of February 2024). As a result of scientific research, the UzFirewall-next generation firewall software tool analyzed 9456 packets out of 11230 packets in the system within 1 hour, and the packet filtering efficiency was 84%;

the UzFirewall-next generation firewall software tool was developed on the basis of the proposed methods, algorithms and architectures and it was implemented into the practical activity of the corporate network of "Innovations in Cybernetics IT Park" LLC (the reference of the Cybersecurity Center of the state unitary enterprise No. 03-18-01/410 of February 2024). During the test, this tool detected a total of 9,764 events for 1 hour, and identified 546 attacks and 22 false alarms. Then it can be seen that the tool has a false alarm rate of 4%. Moreover, the obtained indicators allow to determine how quickly the system responds to and blocks attacks, evaluate response times over time to reveal trends in the appearance of attacks and changes in the response times of cross-network screens, and improve network security strategies and processes;

the UzFirewall-next generation firewall software tool was developed on the basis of network traffic filtering method and algorithms for minimizing the processing time of network packet rules that it was implemented into the practical activity of the corporate network of the "Center for the Development of Information and Communication Technologies" under the State Committee for the roads (the reference of the "Center for the Development of Information and Communication Technologies" under State Committee for the roads of the Republic of Uzbekistan No. 24/32 of April 2024). As a result of the research, the UzFirewall-next generation firewall software tool allowed it possible to detect approximately 92% of all current network anomalies according to the sensitivity criterion and approximately 84% of all events classified as network anomalies according to the accuracy criterion;

the UzFirewall-next generation firewall software tool was developed on the basis of protection algorithms for protecting web resources from malicious bots and suspicious packets that it was implemented in the practical activity of the corporate network of the Center for the Development of "Safe City" Systems of the Ministry of Internal Affairs of the Republic of Uzbekistan (reference of the Center for the Development of "Safe City" Systems of the Ministry of Internal Affairs of the Republic of Uzbekistan No.03/419 of April 2024). During the test, the UzFirewall-next generation firewall software tool, based on the Gaussian distribution function, found that the probability of network packets belonging to normal traffic is approximately 0.7% and the probability of belonging to offensive traffic is 0.2%. This evaluation allowed it possible to quantify the effectiveness of network traffic classification methods and determine their performance.

Structure and volume of the dissertation. The composition of the dissertation consists of an introduction, five chapters, a conclusion, a list of used literature and appendices. The length of the dissertation is 184 pages.

E'LON QILINGAN ISHLAR RO'YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I bo'lim (I часть; I part)

1. Gulomov Sherzod Rajaboevich, Ganiev Abdukhalil Abdujalilovich. Methods and models of protecting computer networks from un-wanted network traffic. International Journal of "Engineering & Technology". Vol. 7, No 4, (2018). Science Publishing Corporation, RAK Free Trade Zone, RAK FTZ Business Park, Business Centre 4, Al Mamourah Area, P.O. Box: 487447, UAE. – P.2541-2545 (Scopus, DOI: https://doi.org/10.14419/ijet.v7i4.14744; IF = 0.2).

2. Gulomov Sherzod, Abdullaev Dilmurod, Malikova Nodira, Akhmedova Husniya. Construction of Schemes, Models and Algorithm for Detection Network Attacks in Computer Networks. International Journal of "Innovative Technology and Exploring Engineering (IJITEE)". ISSN: 2278-3075. Volume 8, Issue 12, 2019. – P.2234-2240 (Scopus, DOI: 10.35940/ijitee.L2481.1081219; IF = 1).

3. Gulomov Sh.R., Kadirov M.M., Karimova N.A., Raximjonov U.Sh. Building a k-means algorithm to reduce false positives when determining a network attacks. International Journal of "Advanced Research in Science, Engineering and Technology". Vol. 6, Issue 10, 2019. – P.11107-11111 (05.00.00; № 8).

4. Gulomov Sherzod Rajaboevich, Xoshimova Charos Saidaminovna, Ganiyeva Toxira Irkinovna, Djurayeva Shoxista Tagirovna. Analysis of Methods for Measuring Available Bandwidth and Classification of Network Traffic. International Journal of "Emerging Trends in Engineering Research". Volume 8, No.6, June 2020. –P.2753-2759 (OAK(40) ResearchGate, DOI: https://doi.org/10.30534/ijeter/2020/).

5. Karimov Madjit Malikovich, Gulomov Sherzod Rajaboevich. IP-Traffic classification model based on machine learning ways. Chemical Technology, Control and Management. Volume 2020, Issue 5 Special issue 5-6, – P. 123-128 (05.00.00; №12; DOI: https://doi.org/10.34920/2020.5-6).

6. Гуломов Ш.Р., Насруллаев Н.Б., Абдурахмонов А.А., Азизова З.И. Оценка и применение алгоритмов машинного обучения для систем обнаружения и предотварешение вторжений. "Муҳаммад ал-Хоразмий авлодлари" илмий-амалий ва ахборот-таҳлилий журнали. № 4 (14), 2020. – С.21-27 (05.00.00; №10).

7. Sh.R.Gulomov. Risk detection model in packet filtering rules based on Fuzzy Petri Net. "Technical science and Innovation Journal", 2021, №3. – P.181-189 (05.00.00; №16).

8. Gulomov Sherzod Rajaboevich, Malikova Nodira Turgunovna, Qurbonova Kabira Erkinovna, Arzieva Jamila Tileubaevna. A method to improve the quality of service and overcome the loss of network packets. International Conference on "Information Science and Communications Technologies ICISCT 2021". Tashkent, Uzbekistan-2021. –3p. (OAK раёсатининг қарори 30.09.2021 йил №525).

9. Karimov Madjit Malikovich, Gulomov Sherzod Rajaboevich, Tashmatova

Shaxnoza Sobirovna, Elmuradov Temurmalik. Differentiated Services Code Point (DSCP) Traffic Filtering Method to Prevent Attacks. International Conference on "Information Science and Communications Technologies ICISCT 2021". Tashkent, Uzbekistan-2021. – 4p. (OAK rayosatining qarori 30.09.2021-yil №525).

10. Gulomov Sherzod Rajaboevich, Nasrullaev Nurbek Baxtiyorovich, Toshev Sanjar Komilovich. A model for preventing malicious traffic in DNS servers using machine learning. International Conference on "Information Science and Communications Technologies ICISCT 2021". Tashkent, Uzbekistan-2021. – 4p. (OAK rayosatining qarori 30.09.2021-yil №525).

11. Gulomov Sherzod, Abdurakhmonov Abduaziz Abdugafforovich, Azizova Zarina Ildarovna. Development a Model of a Network Attack Detection in Information and Communication Systems. Journal of "Advances in Information Technology". Vol. 13, No. 4, August 2022. –P.312-319 (Scopus, DOI: 10.12720/jait.13.4.312-319; Q3).

12. G'ulomov Sh.R. Veb-hujumlardan trafikni veb-filtrlash arxitekturasi. Multidisciplinary Scientific Journal "Innovative Development in Educational Activities". Volume 2, Issue 18, 2023. – B.229-239 (OAK (23) Scientific Journal Impact Factor 5.938).

13. Gulomov Sherzod Rajaboevich, Tashev Sarvar Norboboevich, Kushiev Bakhodir Khabibjonovich. Architecture for optimizing traffic filtering rules. 2023 International Conference on "Information Science and Communications Technologies (ICISCT)". Tashkent, Uzbekistan-2023. – 4p. (OAK rayosatining qarori 29.09.2023-yil №431).

14. Gulomov Sherzod Rajaboevich, Kadirov Mir-Xusan Mirpulatovich, Tashev Sarvar Norboboevich. The structure of tracking suspicious packets in network traffic. 2023 International Conference on "Information Science and Communications Technologies (ICISCT)". Tashkent, Uzbekistan-2023. –4p. (OAK rayosatining qarori 29.09.2023-yil №431).

15. G'ulomov Sh.R. Tarmoqdagi zararli trafik turlari va ularni aniqlash. Multidisciplinary Scientific Journal, "Innovative Development in Educational Activities". Volume 2, Issue 24. 2023. – B.424-432 (OAK (23) Scientific Journal Impact Factor 5.938).

II bo'lim (II часть; II part)

16. G'ulomov Sherzod Rajaboyevich, Ibrohimov Azizbek Ravshanbek o'g'li. Korporativ tarmoq xavfsizligi muammolarini yechish yo'llari. "Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари" Республика миқёсидаги илмий-техник конференция. Тошкент-2018. – Б.163-165.

17. M.M. Karimov, Sh.R.Gulomov. Analysis challenge protection of information from attacks and construction of a formal model for protecting network traffic. Tenth World Conference "Intelligent Systems for Industrial Automation-WCIS-2018". Tashkent, Uzbekistan. 2018. – P.84-88.

18. G'ulomov Sherzod Rajaboyevich, Yusupov Zarif Karamat o'g'li. Tarmoq

zaifliklari tahlili va hujumlarni amalga oshirish usullari. "Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари" Республика миқёсидаги илмий-техник конференция. Тошкент-2018. – Б.62-64.

19. Гуломов Ш.Р., Шамшиева Б.М. Моделирование атак для активного анализа уязвимостей компьютерных сетей. "Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари" Республика миқёсидаги илмий-техник конференция. Тошкент-2018. – С.112-116.

20. Гуломов Шерзод Ражабоевич. Применение математических моделей для оценки Flood атак. "Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари" Республика миқёсидаги илмий-техник конференция. Тошкент-2018. – С.300-304.

21. Karimov Madjid Malikovich, Gulomov Sherzod Rajaboevich, Yusupov Bokhodir Karamatovich. Method of constructing packet filtering rules. International Conference on "Information Science and Communications Technologies: Applications, Trends and Opportunities (ICISCT)". Tashkent, Uzbekistan-2019. – 4p (DOI: 10.1109/ICISCT47635.2019.9011933).

22. Gulomov Sherzod, Saparova Gaukhar. Development of Specialized Method for Increasing the Level of Security on Information and Communication Systems. International Journal of "Innovative Technology and Exploring Engineering (IJITEE)". Volume-9, Issue-2, 2019. – P.1821-1826.

23. Bozorov Suhrobjon Mumin o'g'li, Karimov Madjid Malikovich, Kwangjo Kim, Gulomov Sherzod Rajaboyevich. ANN based DDOS attack detection on computer networks. Сборник статей по материалам XXIII международной научно-практической конференции. Технические науки: проблемы и решения. № 5 (21). Москва-2019. – P.109-115.

24. Yusupov Sabirjan Yusupdjanovich, Gulomov Sherzod Rajaboevich. Improvement the schemes and models of detecting network traffic anomalies on computer systems. 2020 IEEE 14th International Conference on "Application of Information and Communication Technologies (AICT)". Tashkent, Uzbekistan-2020. –5p. (DOI: 10.1109/AICT50176.2020.9368781).

25. Gulomov Sherzod Rajaboevich, Karimova Dilbar, Akbarova Shokhida Azatovna, Qosimova Gulnora Ismoilovna. Comparative Analysis of Methods Content Filtering Network Traffic. International Journal of "Emerging Trends in Engineering Research". Volume 8, No.5, May 2020. – P.1561-1569.

26. M.M. Karimov, Sh.R.Gulomov, S.M. Khamdamova. Modeling the one-way network packet delay. Тези доповідей 9-ї Міжнародної наукової конференції "Сучасні проблеми математичного моделювання, прогнозування та оптимізації". Кам'янець-Подшьський. 2020. – P.51-52.

27. Gulomov Sherzod Rajaboevich, Isoqov Fayozbek Faxriddinovich. Analysis of the features of transmission and parsing of network traffic. "Ижтимоий соҳаларни рақамлаштиришда инновацион технологияларнинг ўрни ва аҳамияти". Республика илмий-амалий анжумани маърузалар тўплами. Қарши-2020. – P.335-339.

28. M.M.Karimov, A.A.Ganiev, Sh.R.Gulomov. Схема обнаружения аномалий сетевого трафика в информационно-коммуникационных системах. "Иқтисодиёт тармоқларининг инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти". Республика илмий-техник анжуманининг маърузалар тўплами, 2-қисм. Тошкент-2021. – C.237-239.

29. G'ulomov Sh.R., Murodov O.O., Ishmuratova M.R. An approach to determining ICMP-Flood attacks in multi Web-servers. "Axborot xavfsizligi sohasida raqamlashtirish muammolari va istiqbollari" Respublika ilmiy-amaliy anjumani materiallari to'plami. Toshkent-2022. – P.41-44.

30. Gulomov Sherzod Rajaboevich, Mirzaeva Malika Bakhadirovna, Iminov Abdurasul Abdulatipovich. Port-Knocking Method for Enhancing Network Security. 2022 International Conference on "Information Science and Communications Technologies (ICISCT)". Tashkent, Uzbekistan-2022. – 4p.

31. Gulomov Sherzod Rajaboevich, Kadirov Mir-Xusan Mirpulatovich, Arzieva Jamila Tileubaevna. Method for implementing traffic filtering in SDN networks. 2022 International Conference on "Information Science and Communications Technologies (ICISCT)". Tashkent, Uzbekistan-2022. – 3p.

32. G'ulomov Sh.R., Sayfullayev Sh.B. Tarmoq trafigini filtrlashning texnik usullari. "Axborot xavfsizligi sohasida raqamlashtirish muammolari va istiqbollari" Respublika ilmiy-amaliy anjumani materiallari to'plami. Toshkent-2022. – B.44-47

33. Sh.R.G'ulomov. Tarmoq trafigida anomaliyalar va noqonuniy harakatlarni aniqlash bosqichlari. "Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari" Respublika ilmiy-amaliy anjumani ma'ruzalar to'plami. Toshkent-2023. – B.19-24.

34. Sh.R.G'ulomov. Uzfirewall-next generation firewall apparat-dasturiy vositasining funksional strukturasi. «Xalq xo'jaligi sohasida ilg'or texnologiyalar tatbiqi muammolari» mavzusidagi hududiy ilmiy-texnik konferensiya. Nukus-2023. – B.136-140.

35. G'ulomov Sherzod Rajaboyevich. UZFirewall-next generation. O'zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro'yxatdan o'tkazilganligi to'g'risidagi guvohnoma № DGU 27073. Toshkent, 29.08.2023.

36. G'ulomov Sherzod Rajaboyevich. IP-paketlarni filtrlashning dasturiy paketi. O'zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro'yxatdan o'tkazilganligi to'g'risidagi guvohnoma № DGU 30421. Toshkent, 04.12.2023.

37. G'ulomov Sherzod Rajaboyevich. Islomov Dostonbek Uktamjon-o'g'li. Trafikni filtrlash qoidalari ortiqchaligini aniqlovchi dasturiy paket. O'zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro'yxatdan o'tkazilganligi to'g'risidagi guvohnoma № DGU 32863. Toshkent, 26.01.2024.

Avtoreferat "Muhammad al-Xorazmiy avlodlari" ilmiy jurnali tahririyatida tahrirdan o'tkazildi va o'zbek, rus va ingliz tillaridagi matnlarini mosligi tekshirildi.

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog'i: 4,25. Adadi 100 dona. Buyurtma № 29/24.

Guvohnoma № 851684.
«Tipograff» MCHJ bosmaxonasida chop etilgan.
Bosmaxona manzili: 100011, Toshkent sh., Beruniy ko'chasi, 83-uy.