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

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

SADIKOV SHUXRAT MUXAMADJANOVICH

KORPORATIV TARMOQ FOYDALANUVCHILARINING TAQSIMLANGAN MA'LUMOTLAR BAZASI XAVFSIZLIGINI TA'MINLASH USULLARI VA ALGORITMLARI

05.01.05-Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI DOKTORI (DSc) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2023

UDK 004.056.57

Doktorlik (DSc) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата докторской (DSc) диссертации

Contents of the abstract of Doctoral (DSc) dissertation

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

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

SADIKOV SHUXRAT MUXAMADJANOVICH

KORPORATIV TARMOQ FOYDALANUVCHILARINING TAQSIMLANGAN MA'LUMOTLAR BAZASI XAVFSIZLIGINI TA'MINLASH USULLARI VA ALGORITMLARI

05.01.05-Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

**TEXNIKA FANLARI DOKTORI (DSc)
DISSERTATSIYASI AVTOREFERATI**

Toshkent – 2023

Texnika fanlari doktori (DSc) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2023.3.DSc/T655 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:	**Maxkamov Baxtiyor Shuxratovich** iqtisodiyot fanlari doktori, professor
Rasmiy opponentlar:	**Kerimov Kamil Fikratovich** texnika fanlari doktori, dotsent
	Jurayev Gayrat Umarovich fizika-matematika fanlari doktori, professor
	Primova Xolida Anarboyevna texnika fanlari doktori, dotsent
Yetakchi tashkilot:	**Islom Karimov nomidagi Toshkent davlat texnika universiteti**

Dissertasiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.02 raqamli Ilmiy kengashning 2023 yil «31» 10 da soat 11:00 dagi majlisida bo‘lib o‘tadi. (Manzil: 100202, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43; e-mail: tuit@tuit.uz).

Dissertasiya bilan Toshkent axborot texnologiyalari universitetining Axborot-resurs markazida tanishish mumkin (284 raqam bilan ro‘yxatga olingan). (Manzil: 100202, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43).

Dissertasiya avtoreferati 2023 yil “20” 10 da tarqatildi.
(2023 yil «19» 10 dagi 4 raqamli reyestr bayonnomasi).

D.Y. Irgasheva
Ilmiy darajalar beruvchi ilmiy kengash raisi o‘rinbosari, t.f.d., professor

E.Sh. Nazirova
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, t.f.d., professor

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

KIRISH (doktorlik dissertasiyasi avtoreferati (DSc))

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahon iqtisodiyotining bugungi holati va rivojlanish istiqbollari ustuvor darajada raqamli va sun'iy intellekt texnologiyalariga asoslanishi sharoitida korxonalar ma'lumotlarini qabul qilish, qayta ishlash, saqlash va axborotni uzatishning boshqarish tizimlarini samarali ta'minlashda kibertahdidlar va kiberhujumlardan samarali himoyalash muhim muammolardan biri bo'lib qolmoqda. "Kaspersky" kompaniyasining statistik ma'lumotlarga qaraganda, ma'lumotlar bazasiga bo'ladigan hujumlar soni 2020-yilda barcha hujumlarning 27 foizni tashkil etgan bo'lsa, oxirgi uch yilda bu ko'rsatgich 2,8 martaga ortib, 2023-yilda umumiy hisobda kiberhujumlarning 75,6 foizni tashkil qilgan[1]. Bugungi kunda jahonda axborot tizimlarini kibertahdid va kiberhujumlardan samarali himoyalash tizimini yaratishda axborotlar yaratilishining asosini tashkil qiluvchi korxona ma'lumotlar bazasini ishonchli himoyalashning dasturiy-texnologik ta'minotini tashkil qilish, taqsimlangan ma'lumotlar bazasini himoyalash tizimining samaradorligini oshirish, korporativ tarmoq foydalanuvchilarning taqsimlangan ma'lumotlar bazasida tarmoq hujumlarini ishonchli himoyalash, tahdidlarni aniqlashning samarali usullari va algoritmlarini qo'llash kabi chora-tadbirlarga alohida ahamiyat qaratilmoqda.

Jahonda korxonalarning korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasi, taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usullari va algoritmlarini takomillashtirish hamda taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash usul va algoritmlarini ishlab chiqishga qaratilgan ilmiy loyihalar ustuvor darajada amalga oshirilmoqda. Bu borada, taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarini himoyalash, ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish hamda taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modellarini ishlab chiqish, taqsimlangan ma'lumotlar bazasida zaifliklarni va korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usullari va algoritmlarini ishlab chiqish kabi mavzulardagi tadqiqotlarga alohida e'tibor qaratilmoqda.

Yangi O'zbekistonni barpo etish jarayonida mamlakatimiz strategik taraqqiyotining ustuvor yo'nalishlaridan biri sifatida itisodiyotni raqamlashtirish belgilangan holda "Raqamli O'zbekiston – 2030" strategiyasi doirasida axborot-kommunikatsiya texnologiyalari sohasini sifat jihatdan yangi bosqichga olib chiqish, axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish hamda tashkiliy va dasturiy-texnologik asoslarini zamonaviy talablarga ko'ra mustahkamlash kabilar yuzasidan keng qamrovli dasturiy chora-tadbirlar amalga oshirilmoqda.[2] Mazkur vazifalar ijrosini samarali tashkil qilishda, jumladan, taqsimlangan ma'lumotlar bazasida

---

[1] https://securelist.ru/it-threat-evolution-q1-2023-pc-statistics/107526/
https://securelist.ru/it-threat-evolution-q1-2023/107467/
https://securelist.ru/it-threat-evolution-q1-2023-mobile-statistics/107514/

[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

tashkilot aktivlari va resurslarni himoyalash, ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish hamda taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modellarini ishlab chiqish, zaifliklarni va korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini samarali aniqlash kabi yo'nalishidagi tadqiqotlarni chuqurlashtirish maqsadga muvofiq.

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 Qarori, 2018 yil 19 fevraldagi PF-5349-son "Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to'g'risida"gi Farmonlari, 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 va 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, hamda mazkur faoliyatga tegishli boshqa meyoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya tadqiqoti 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]**.** Jahonda korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash usullari va algoritmlarini ishlab chiqish va takomillashtirishga qaratilgan ilmiy tadqiqotlar, jumladan quyidagi yetakchi ilmiy markazlar va oliy o'quv yurtlarida amalga oshirilmoqda: Buyuk Pyotr nomidagi Sankt-Peterburg politexnika universiteti va N.E.Bauman nomidagi Moskva davlat texnika universiteti (Rossiya), Dongguk universiteti (Janubiy Koreya), Gonkong fan va texnologiya universiteti (Xitoy), Shvetsariya Federal texnologiya insituti (Shvetsariya), Massachusets texnologiya instituti (AQSH), Janubiy Koreya ilmiy va texnologiya ilmiy instituti (Janubiy Koreya), Tokio texnologiya instituti (Yaponiya), Myunxen texnika universiteti (Germaniya), Delft texnologiya universiteti (Niderlandiya), Xitoy fan va texnologiya universiteti (Xitoy)da va respublikamizda Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Mirzo Ulug'bek nomidagi O'zbekiston milliy 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 korxonasi (O'zbekiston Respublikasi).

[3] Dissertatsiya mavzusi bo'yicha ilmiy tadqiqotlar sharhi https://www.researchgate.net, www.elsevier.com, http://www.machinelearning.ru, http://www.bmstu.ru, https://habr.com va boshqa manbalar asosida shakllantirilgan.

Jahonda taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarni himoyalash, ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish hamda taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modellarini ishlab chiqish bo'yicha, jumladan quyidagi ilmiy natijalar olingan: korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasi, taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usullari ishlab chiqilgan (Shvetsariya Federal texnologiya insituti (Shvetsariya), Massachusets texnologiya instituti (AQSH)), taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash algoritmlari ishlab chiqilgan (Dongguk universiteti (Janubiy Koreya), Delft texnologiya universiteti (Niderlandiya)), korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usullari va algoritmlari ishlab chiqilgan (Massachusets texnologiya instituti (AQSH), N.E.Bauman nomidagi Moskva davlat texnika universiteti (Rossiya)).

Dunyoda korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash usullari va algoritmlarini takomillashtirish va ishlab chiqish bo'yicha, jumladan quyidagi yo'nalishlarda ustuvor darajada tadqiqotlar olib borilmoqda: korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasi, taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usullari va algoritmlarini real vaqt rejimini e'tiborga olgan holda takomillashtirish; taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash usul va algoritmini foydalanuvchilarning vakolatlariga ko'ra ishlab chiqish; taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarni himoyalash, ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish hamda taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modellarini tashkilotning korporativ tarmog'idagi aktivlari va resurslarini e'tiborga olgan holda ishlab chiqish; tizimdagi zaifliklarni va korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usullari va algoritmlarini sathlarga ajratish asosida takomillashtirish.

Muammoning o'rganilganlik darajasi. Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasini himoyalashda diskret matematika, graflar nazariyasi, tasodifiy jarayonlarni modellashtirish, mashinali o'qitishga asoslangan modellar va shunga o'xshash intellektual usullar asosida zamonaviy himoya mexanizmlarini uchun yangi usullar va algoritmlarni tadbiq etish bo'yicha M. Malik, T. Patel, I. Ghafir, J. Saleem, M. Hammoudeh, P. K. Paul, P. S. Aithal, S. B. Sadkhan, va boshqa chet ellik olimlar tomonidan ilmiy izlanishlar olib borilmoqda. Taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarni himoyalash, ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish hamda taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modellarini ishlab chiqishda zamonaviy usullarni qo'llagan holda A. Suwalka, S. Kumar, J. C. Ogbonna, F. O. Nwokoma, X.Wang, L.Zhou, Yuan, V. Sharma, W. Lee. kabi olimlar tomonidan ilmiy izlanishlar olib borilgan va hozirda hamda ular boshchiligidagi ilmiy maktablari tomonidan davom ettirilmoqda. Bundan tashqari, InfoWatch, ideco, CyberBit, Juniper Networks, Fortinet, Garda

Texnologii va Cloud Networks tashkilotlari tomonidan taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlashga hamda korxonaning butun axborot tizimida axborotni himoyalashning dasturiy-apparat vositalarini ishlab chiqishga qaratilgan ilimiy-amaliy muhandislik-tadqiqot ishlari olib borilmoqda.

O'zbekistonda T.F.Bekmuratov, S.K.Ganiyev, M.M.Karimov, D.Y.Irgasheva N.A. Ignatev, G.Jurayev, R.X.Xamdamov, K.F.Kerimovlar boshchiligidagi ilmiy jamoalar tomonidan korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasidagi zaifliklarni aniqlash va korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usullari va algoritmlarini ishlab chiqish bo'yicha ilmiy izlanishlar olib borilgan.

Shu bilan birga taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarni himoyalash, ruhsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish hamda taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modellarini ishlab chiqish va korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasi, taqsimlangan ma'lumotlar bazasida resuslarni zaxira nusxalash usullari va algoritmlarini takomillashtirish hamda taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash usul va 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" hamda "Bo'lak-polinomial bazislarda signallar va tasvirlarga raqamli ishlov berishning intellektual dasturiy-texnik tizimlarini yaratishning nazariy metodologik asoslari" mavzusidagi loyiha doirasida bajarilgan.

Tadqiqotning maqsadi taqsimlangan ma'lumotlar bazasini himoyalash tizimining samaradorligini oshirishga imkon beruvchi korporativ tarmoq foydalanuvchilarning taqsimlangan ma'lumotlar bazasida zaifliklar va tarmoq hujumlarini aniqlashning natijador usullari va algoritmlarini ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

korporativ tarmoqda ma'lumotlar bazasiga bo'ladigan tarmoq hujum turlari va ularni tasniflanishini qiyosiy tahlil qilish;

korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasini ishlab chiqish;

taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usul va algoritmini ishlab chiqish;

taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarni himoyalash hamda ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish modellarini ishlab chiqish;

taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modelini ishlab chiqish;

taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash usul va algoritmi ishlab chiqish;

taqsimlangan ma'lumotlar bazasida zaifliklarni aniqlash usul va algoritmini ishlab chiqish;

korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usul va algoritmini ishlab chiqish.

Tadqiqotning obyekti sifatida O'zbekiston Respublikasi korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasini himoyalash jarayoni olingan.

Tadqiqotning predmetini korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasida zaiflik va tarmoq hujumlarini aniqlash va bartaraf etish usullari va algoritmlari tashkil etadi.

Tadqiqotning usullari. Tadqiqot jarayonida ehtimollar nazariyasi, to'plamlar nazariyasi, diskret matematika, tasodifiy jarayonlarni modellashtirish, ma'lumotlar bazasini himoyalash, obyektga yo'naltirilgan dasturlash va boshqa usullardan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

taqsimlangan ma'lumotlar bazasi tizimlarini integratsiyalash uchun ishlab chiqilgan arxitektura (ANSI/SPARC: American National Standards Institute, Standards Planning And Requirements Committee) markazlashtirilgan MBBTlari uchun umumiy komponentga ega bo'lgan korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasini arxitekturasi global koseptual sxemaga ko'ra takomillashtirilgan;

ma'lumotlar bazasidagi ma'lumotlarni to'liq, o'sib borish va differensial zaxiralash imkoniyatidan foydalangan holda real vaqt rejimida taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usuli va algoritmi ishlab chiqilgan;

qarorlarini qo'llab-quvvatlashning dinamik ekspert tizimlariga asoslangan holda foydalanish darjasiga ko'ra himoyalangan aktivlarini boshqarish va axborotni himoyalash tizimining resurslarini boshqarish jarayonida taqsimlangan ma'lumotlar bazasidagi ma'lumotlarining o'zaro ta'siri modellari ishlab chiqilgan;

tashkilotda foydalanilayotgan taqsimlangan ma'lumotlar bazasidagi ma'lumotlardan foydalanishni boshqarish mexanizmlaridan kelib chiqib, foydalanuvchi vakolatlarini foydalanishni boshqarish aspektlari asosida taqsimlangan ma'lumotlar bazasida ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish modellari takomillashtirilgan;

taqsimlangan ma'lumotlar bazasi xavfsizligi va axborotni himoyalash bo'yicha ichki va tashqi huquqiy hujjatlarning talablaridan kelib chiqqan holda, umumiy resurslarning ichki va tashqi parametrlariga ko'ra ekspertlar guruhining axborotni himoya qilish tizimi va himoya qilish obektlari bo'yicha xulosasi asosida taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modeli ishlab chiqilgan;

ma'lumotlar bazasiga foydalanuvchilar tomonidan yuborilgan so'rovlarga mos javoblarni kerakli jadvallardan qidirishda chiziqli, ikkilik va interpolyatsiya qidiruv

algoritmlarini qo'llash asosida axborot tizimi muhitiga ko'ra taqsimlangan ma'lumotlar bazasidagi zaifliklarni aniqlash usuli va algoritmi ishlab chiqilgan;

korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasida aktivlar, resurslar, xodimlar, uchinchi shaxs, hujum, tahdid, zaiflik va risk darajalariga vazn tushunchasini kiritish asosida korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini aniqlash usuli va algoritmi takomillashtirilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

ruxsatlarni boshqarishning RBAC usulidagi mavjud kamchiliklarni ruxsatlarni boshqarishning ABAC usullidagi atributlari orqali takomillashtirish natijasida taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash usuli va algoritmi ishlab chiqilgan;

taqsimlangan ma'lumotlar bazasining mijoz-server arxitekturasida axborot xavfsizligi komponentalarining joylashuv sxemasidan foydalangan holda resuslarni zaxira nusxalash va xavfsizlikni ta'minlash dasturiy vositasi ishlab chiqilgan;

ruxsatlarni boshqarishning RBAC usulidagi mavjud kamchiliklarni ruxsatlarni boshqarishning ABAC usulidagi atributlari orqali takomillashtirish natijasida ishlab chiqilgan usul va algoritmdan foydalanib, foydalanuvchilarning vakolatlarini belgilash va rollarini taqsimlashning dasturiy vositasi ishlab chiqilgan;

ma'lumotlar bazasiga foydalanuvchilar tomonidan yuborilgan so'rovlarga mos javoblarni kerakli jadvallardan qidirishda chiziqli, ikkilik va interpolyatsiya qidiruv algoritmlarini qo'llagan holda ishlab chiqilgan usul va algoritmdan foydalanib, taqsimlangan ma'lumotlar bazasidagi zaifliklarni aniqlashning dasturiy vositasi ishlab chiqilgan;

korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasida aktivlar, resurslar, hodimlar, uchinchi shaxs, hujum, tahdid, zaiflik va risk darajalariga vazn tushunchasini kiritish orqali ishlab chiqilgan usul va algoritmdan foydalanib, taqsimlangan ma'lumotlar bazasiga nisbatan bo'ladigan tarmoq hujumlarini aniqlashning dasturiy vositasi ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi. Tadqiqotda qo'llanilgan yondashuv va usullarning maqsadga muvofiqligi, ma'lumotlarning rasmiy manbalardan, jumladan Kiberxavfsizlik markazi davlat unitar korxonasi va O'zbekiston Respublikasi Raqamli texnologiyalar vazirligining statistik ma'lumotlaridan olingani hamda tegishli xulosa va takliflarning mutasaddi tashkilotlar tomonidan amaliyotga joriy etilganligi bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasi, taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usullari va algoritmlarini real vaqt rejimida foydalanish darjasiga ko'ra takomillashtirilgani, taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash xususan, taqsimlangan ma'lumotlar bazasida zaifliklarni va korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usullari va algoritmlarini ishlab chiqish va takomillashtirish

hamda tashkilotning korporativ tarmog'ida axborotni himoyalash tizimlarini rivojlantirishga xizmat qiladi.

Tadqiqot natijalarining amaliy ahamiyati taklif etilgan usullar va algoritmlar asosida ishlab chiqilgan dasturiy ta'minot yordamida tashkilot faoliyat turiga ko'ra korporativ tarmoq foydalanuvchilarning taqsimlangan ma'lumotlar bazasidagi zaifliklarni aniqlash hamda ma'lumotlar bazasiga nisbatatan bo'ladigan tarmoq hujumlarini aniqlash va korxonaning butun axborot tizimida axborot xavfsizligini ta'minlash tizimini avtomatlashtirishga ko'maklashishi hamda olingan natijalarni qo'llash himoya obektida zaifliklarni muhit darajasida (server, mijoz, baza) aniqlash bilan bir qatorda, ma'lumotlar bazasini tarmoq hujumlaridan himoyalashda sarflanadigan tashkilot resurslarini qisqartirish va ulardan samarali foydalanish imkonini berishi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash usullari hamda dasturiy vositalari bo'yicha olingan ilmiy natijalar asosida:

taqsimlangan ma'lumotlar bazasi tizimlarini integratsiyalash uchun ishlab chiqilgan arxitektura (ANSI/SPARC: American National Standards Institute, Standards Planning And Requirements Committee) markazlashtirilgan MBBTlari uchun umumiy komponentga ega bo'lgan korporativ tarmoq foydalanuvchilari taqsimlangan ma'lumotlar bazasining arxitekturasi bo'yicha ishlab chiqilgan dasturiy vosita "Kiberxavfsizlik markazi" davlat unitar korxonasining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2023-yil 18-avgustdagi 33-8/5665-son ma'lumotnomasi). Ilmiy tadqiqot natijasida taqsimlangan ma'lumotlar bazasida zaifliklarni aniqlash usuli asosida ishlab chiqilgan dasturiy vosita korxonaning taqsimlangan ma'lumotlar bazasida 5 ta asosiy turdagi 77 ta zaifliklarni 97,5 foiz aniqlik qayd etgan holda aniqlash imkonini bergan;

ma'lumotlar bazasidagi ma'lumotlarni to'liq, o'sib borish va differensial zaxiralash imkoniyatidan foydalangan holda real vaqt rejimida taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usuli va algoritmi asosida ishlab chiqilgan dasturiy vosita "Kiberxavfsizlik markazi" davlat unitar korxonasining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2023-yil 18-avgustdagi 33-8/5665-son ma'lumotnomasi). Ilmiy tadqiqot natijasida korxonaning taqsimlangan ma'lumotlar bazasiga bo'ladigan 9108 ta tarmoq hujumlaridan 8935 tasini 98,1 foiz aniqlik qayd etgan holda aniqlash imkonini bergan. Ushbu dasturiy vositaning samaradorligini aniqlash maqsadida amaldagi dasturiy vositalar bilan solishtirish natijasida boshqa dasturiy vositalarga nisbatan tarmoq hujumlarini aniqlash tezligi 1,8 ms tezligi yuqoriligi va tizimning yolg'on ishga tushish holatlari soni 1,6 marta kamligi aniqlangan;

qarorlarini qo'llab-quvvatlashning dinamik ekspert tizimlariga asoslangan holda foydalanish darjasiga ko'ra himoyalangan aktivlarini boshqarish va axborotni himoyalash tizimining resurslarini boshqarish jarayonida taqsimlangan ma'lumotlar bazasidagi ma'lumotlarining o'zaro ta'siri modellari asosida ishlab chiqilgan dasturiy vosita "UZINFOCOM Davlat axborot tizimlarini yaratish va qo'llab-

quvvatlash bo'yicha yagona integrator" ma'suliyati cheklangan jamiyatining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2023-yil 18-avgustdagi 33-8/5665-son ma'lumotnomasi). Ilmiy tadqiqot natijasida korxonaning taqsimlangan ma'lumotlar bazasida 6 ta asosiy turdagi 76 ta zaifliklarni 98,2 foiz aniqlik qayd etgan holda aniqlash hamda korxonaning taqsimlangan ma'lumotlar bazasiga bo'ladigan 7683 ta tarmoq hujumlaridan 7560 tasini 98,3 foiz aniqlik qayd etgan holda aniqlash imkonini bergan;

tashkilotda foydalanilayotgan taqsimlangan ma'lumotlar bazasidagi ma'lumotlardan foydalanishni boshqarish mexanizmlaridan kelib chiqib, foydalanuvchi vakolatlarini foydalanishni boshqarish aspektlari asosida taqsimlangan ma'lumotlar bazasida ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish modellari asosida ishlab chiqilgan dasturiy vosita "UZINFOCOM Davlat axborot tizimlarini yaratish va qo'llab-quvvatlash bo'yicha yagona integrator" ma'suliyati cheklangan jamiyatining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2023-yil 18-avgustdagi 33-8/5665-son ma'lumotnomasi). Ushbu dasturiy vositaning samaradorligini aniqlash maqsadida amaldagi dasturiy vositalar bilan solishtirish natijasida boshqa dasturiy vositalarga nisbatan tarmoq hujumlarini aniqlash tezligi 2,1 ms tezligi yuqoriligi va tizimning yolg'on ishga tushish holatlari soni 1,7 marta kamligi aniqlangan;

taqsimlangan ma'lumotlar bazasi xavfsizligi va axborotni himoyalash bo'yicha ichki va tashqi huquqiy hujjatlarning talablaridan kelib chiqqan holda, umumiy resurslarning ichki va tashqi parametrlariga ko'ra ekspertlar guruhining axborotni himoya qilish tizimi va himoya qilish obektlari bo'yicha xulosasi asosida taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modeli asosida ishlab chiqilgan dasturiy vosita Elektromagnit moslashuv markazi - "EMMM" davlat unitar korxonasining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2023-yil 18-avgustdagi 33-8/5665-son ma'lumotnomasi). Ilmiy tadqiqot natijasida korxonaning taqsimlangan ma'lumotlar bazasida 6 ta asosiy turdagi 84 ta zaifliklarni 97,1 foiz aniqlik qayd etgan holda aniqlash hamda korxonaning taqsimlangan ma'lumotlar bazasiga bo'ladigan 6574 ta tarmoq hujumlaridan 6417 tasini 97,6 foiz aniqlik qayd etgan holda aniqlash imkonini bergan;

ma'lumotlar bazasiga foydalanuvchilar tomonidan yuborilgan so'rovlarga mos javoblarni kerakli jadvallardan qidirishda chiziqli, ikkilik va interpolyatsiya qidiruv algoritmlarini qo'llash asosida axborot tizimi muhitiga ko'ra taqsimlangan ma'lumotlar bazasidagi zaifliklarni aniqlash usuli va algoritmi asosida ishlab chiqilgan dasturiy vosita Elektromagnit moslashuv markazi - "EMMM" davlat unitar korxonasining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2023-yil 18-avgustdagi 33-8/5665-son ma'lumotnomasi). Ushbu dasturiy vositaning samaradorligini aniqlash maqsadida amaldagi dasturiy vositalar bilan solishtirish natijasida boshqa dasturiy vositalarga nisbatan tarmoq hujumlarini aniqlash tezligi 1,65 ms tezligi yuqoriligi va tizimning yolg'on ishga tushish holatlari soni 1,33 marta kamligi aniqlangan;

korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasida aktivlar, resurslar, xodimlar, uchinchi shaxs, hujum, tahdid, zaiflik va risk darajalariga vazn tushunchasini kiritish asosida korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini aniqlash usuli va algoritmi asosida ishlab chiqilgan dasturiy vosita Radioaloqa, radioeshittirish va televideniye markazi - «RRTM» davlat unitar korxonasining amaliy faoliyatiga joriy qilingan (Raqamli texnologiyalar vazirligining 2023-yil 18-avgustdagi 33-8/5665-son ma'lumotnomasi). Ilmiy tadqiqot natijasida taqsimlangan ma'lumotlar bazasida 4 ta asosiy turdagi 52 ta zaifliklarni 97,8 foiz aniqlik qayd etgan holda aniqlash hamda korxonaning taqsimlangan ma'lumotlar bazasiga bo'ladigan 5462 ta tarmoq hujumlaridan 5304 tasini 97,1 foiz aniqlik qayd etgan holda aniqlash imkonini bergan. Ushbu dasturiy vositaning samaradorligini aniqlash maqsadida amaldagi dasturiy vositalar bilan solishtirish natijasida boshqa dasturiy vositalarga nisbatan tarmoq hujumlarini aniqlash tezligi 1,9 ms tezligi yuqoriligi va tizimning yolg'on ishga tushish holatlari soni 1,8 marta kamligi aniqlangan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 5 ta xalqaro va 7 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o'tkazilgan.

Tadqiqot natijalarining e'lon qilinganligi. Dissertatsiyaning mavzusi bo'yicha jami 28 ta ilmiy ish chop etilgan, jumladan, O'zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarida 13 ta maqola, shulardan, 6 tasi xorijiy va 7 tasi respublika jurnallarida nashr etilgan hamda 3 ta EHM uchun yaratilgan dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, beshta bob, xulosa, foydalanilgan adabiyotlar ro'yxati va ilovalardan iborat. Dissertatsiya hajmi 191 betni tashkil etadi.

DISSERTASIYANING ASOSIY MAZMUNI

Kirish qismida dissertasiya mavzusining dolzarbligi asoslangan, taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash muammolarining qisqacha tahlili keltirilgan, tadqiqot maqsadi va vazifalari aniqlangan. Ilmiy yangiligi ta'riflangan va ish natijalarining amaliy ahamiyati ko'rsatilgan, himoyaga olib chiqiladigan asosiy ilmiy holatlar keltirilgan, tadqiqot natijalarini joriy etish, natijalarning nashr etilishi va dissertasiyaning tuzilishi to'g'risida ma'lumotlar berilgan.

Dissertatsiyaning **"Korporativ tarmoqda taqsimlangan ma'lumotlar bazasini himoya qilish tizimlari tadqiqi"** deb nomalanuvchi birinchi bobida korporativ tarmoqda ma'lumotlar bazasiga bo'ladigan tarmoq hujum turlari va ularni tasniflanishini hamda taqsimlangan ma'lumotlar bazasiga ruxsatsiz harakatlardan asosida kirish va ma'lumotlar bazasi xavfsizligni buzish holatlari va ulardan himoyalanishda foydalaniladigan xavfsizlik modellarining qiyosiy tahlili bilan bir qatorda, butunlikni miqdoriy baholash hamda taqsimlangan ma'lumotlar bazasida axborotni qabul qilish, qayta ishlash va uzatish tizimlarida buzilish holatlarini kamaytirish to'g'risida fikr mulohazalar keltirilgan.

1-jadval.

Ma'lumotlar bazasiga nisbatan bo'ladigan tarmoq hujumlarining qiyosiy tahlili

Hujum nomi / Mezon	SQL inyeksiyasi hujumi	No standart pratokol hujumi	Ping Flooding hujumi	Ma'lumotlarni parchalash hujumi
Tasir darajasi (yuqori, o'rta, past)	yuqori	past	o'rta	past
Onlayn va offlayn (ulanish rejimi ichki va tashqi tarmoq turiga qarab)	onlayn offlayn	onlayn	onlayn	onlayn
MBBT turiga bog'liqligi	bog'liq	bog'liq	bog'liq	bog'liq
Amalga oshirish darajasi (oson, qiyin)	oson	qiyin	oson	qiyin
Konfidensiallikni buzish	+	+	-	+
Butunlikni buzish	+	+	-	+
Foydalanuvchanlikni buzish	+	-	+	+

Ma'lumotlar bazasi xavfsiligini ta'minlash jarayonida ma'lumotlar bazasi xavfsizligi modellari muhim ahamiyat kasb etadi. Axborot xavfsizligini ta'minlashning asosiy yo'nalishlaridan biri, ma'lumotlar bazasi foydalanuvchilarining rollarini belgilab berish hamda ularga taqdim etilgan rollar asosida beriladigan vakolatlardan to'g'ri foydalanishlarini nazorat qilish va zarur hollarda foydalanishni cheklashdir.

Bugungi kunda quyidagi xavfsizlik modellaridan foydalanib kelinmoqda: Xarrison-Ruzzo Ulmanning diskretsion modeli; Goger-Gezinger modeli; Bella-La Padula modeli; Biba modeli; Klark Uilson modeli; Millen modeli; Sazerlend modeli; Xavfsizlikning rolli modeli.

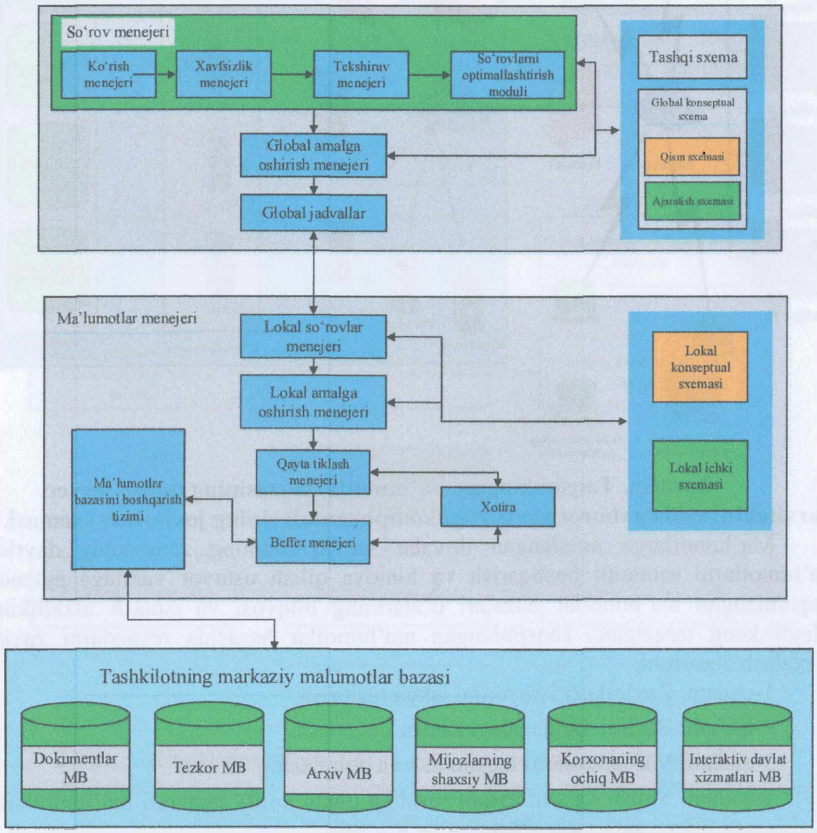
Taqsimlangan ma'lumotlar bazasida axborotni yig'ish, ro'yxatga olish, nazorat qilish, qayta ishlash, aloqa kanallari orqali ma'lumotlarni uzatishning istalgan bosqichlarida ma'lumotlarning yo'qolishi (ularning butunligini buzish) kuzatilishi mumkin. Saqlash vaqtida ma'lumotlar yo'qolishining oldini olish uchun ma'lumot tashish vositalarini mexanik shikastlanishdan va jismoniy ta'sirlardan (masalan, magnit maydonlar) himoya qilish uchun maxsus choralar ko'riladi.

Taqsimlangan ma'lumotlar bazasida ko'p darajali arxitektura, axborotni qayta ishlashning yangi texnologiyalari va ma'lumotlarni taqdim etish shakliga qo'yiladigan yangi talablar bilan bog'liq holda taqsimlangan ma'lumotlar bazasiga bo'ladigan tahdidlar va zaifliklarni aniqlab ularni bartaraf etish zarur.

Dissertatsiyaning **"Taqsimlangan ma'lumotlar bazasida axborot xavfsizligi komponentalari va resurslarni zaxira nusxalash usul va algoritmi"** deb nomalanuvchi ikkinchi bobi korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasini ishlab chiqish bo'yicha fikr mulohazalar va taqsimlangan ma'lumotlar bazasining mijoz-server arxitekturasida axborot xavfsizligi komponentalarining joylashuv sxemasi hamda taqsimlangan ma'lumotlar bazasini himoyalash tizim samaradorligini oshirish bo'yicha takliflar

keltirilgan va taqsimlangan ma'lumotlar bazasida resuslarni zaxira nusxalash usuli va algoritmi ishlab chiqishga bag'ishlangan.

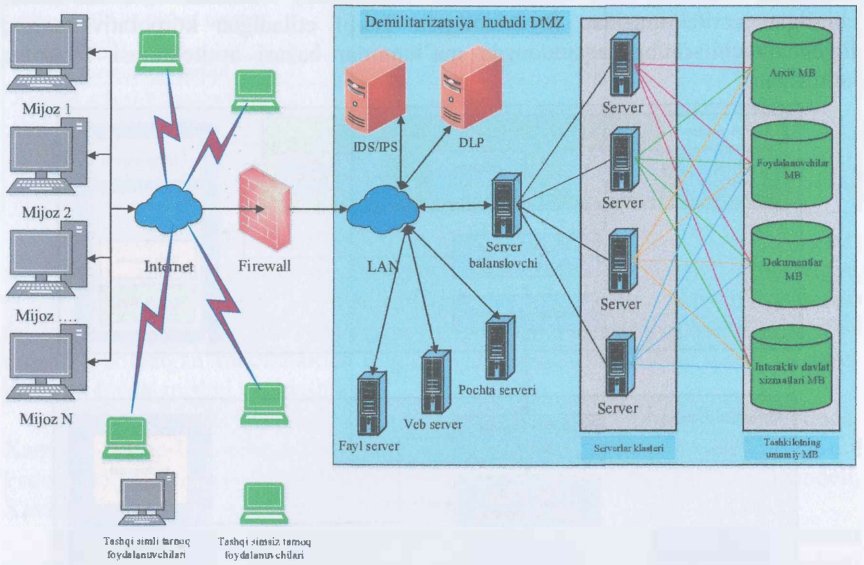
Zamonaviy operatsion tizimlarda har xil turdagi himoyalangan obyektlar soni bir necha o'nlab, himoyalangan axborot oqimlarining har xil turlari soni bir necha yuzga yetishi mumkin. Shuning uchun ham amalga oshirish imkoniyati operatsion tizimda bajarilgan har qanday hujum ko'p jihatdan operatsion tizim arxitekturasi va konfiguratsiyasi bilan belgilanadi. Buni ishlab chiqishda taqsimlangan ma'lumotlar bazasi tizimlari uchun ANSI/SPARC (American National Standards Institute, Standards Planning And Requirements Committee) tomonidan maxsus ishlab chiqilgan arxitekturasidan foydalanilgan. Taklif etiladigan korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasi 1-rasmda keltirilgan.



1-rasm. Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi arxitekturasi.

Taqsimlangan ma'lumotlar bazasi xavfsizligni ta'minlash uchun mijoz-server arxitekturasida axborot xavfsizligi komponentalarini joylashuvi muhim ahamiyat

kasb etadi. Bunga asosiy sabab foydalanuvchilar va ularga kerakli ma'lumotlarni korxonaning ma'lumotlar bazasidan olish jarayonida ularga vakolatlar beriladi. Ushbu vakolatlardan foydalanuvchilarning hammasi ham to'g'ri maqsadda foydalanmaydi. Shuning uchun ham foydalanuvchilarning tizimdan foydalanish holatlarini doimiy kuzatib turish va ruxsatsiz harakatalar aniqlangan vaqtda ularga qarshi reaksiya ko'rsatish mexanizmlarini ishlab chiqish zarur. Shundan kelib chiqib taqsimlangan ma'lumotlar bazasining mijoz-server arxitekturasida axborot xavfsizligi komponentalarining joylashuv sxemasi quyidagicha ko'rinishda bo'ladi (2-rasm).



2.-rasm. Taqsimlangan ma'lumotlar bazasining mijoz-server arxitekturasida axborot xavfsizligi komponentalarining joylashuv sxemasi.

Ma'lumotlarga asoslangan ilovalar va tizimlarning zamonaviy davrida ma'lumotlarni samarali boshqarish va himoya qilish ustuvor vazifaga aylandi. Taqsimlangan ma'lumotlar bazalari o'zlarining miqyosi va ishlash afzalliklari tufayli keng tarqalgan. Taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash algoritmi.

1-qadam. Zaxiralash jarayonini ishga tushirish.

2-qadam. Bo'lim darajasidagi zaxira.

3-qadam. Ma'lumotlarni taqsimlash va oqimlash.

4-qadam. Siqish va shifrlashni hisobga olgan holda samarali ma'lumotlarni uzatish mexanizmlarini joriy qilish.

5-qadam. Qayta tiklanadigan nazorat nuqtalari.

6-qadam. Xatolarni qayta ishlash va tiklash.

7-qadam. To'xtatib turish va davom ettirish funksiyasi.

8-qadam. Tekshirish punktlaridan davom etish.

9-qadam. To'ldirish va tekshirish.

10-qadam. Meta-ma'lumotlarning zaxira nusxasi va kataloglash.

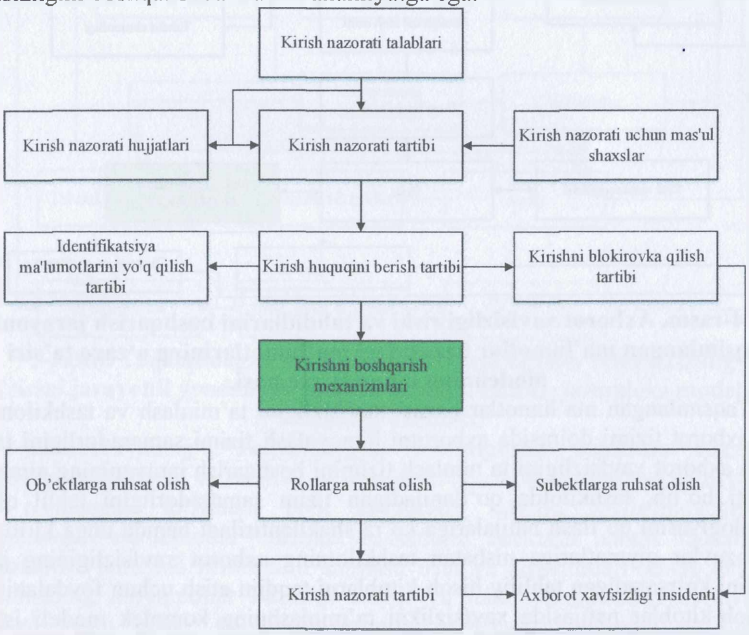
11-qadam. Zaxira hisoboti va monitoring.

12-qadam. Saqlash va boshqarish.

13-qadam. Sinov va tasdiqlash.

Dissertasiyaning **"Korporativ tarmoqdagi taqsimlangan ma'lumotlar bazasida axborotni himoyalash modellari"** deb nomalanuvchi uchinchi bobi taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarni himoyalash va taqsimlangan ma'lumotlar bazasida ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish modellari hamda taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modellarini ishlab chiqishga bag'ishlangan.

Himoyalangan axborot aktivlari, axborot tizimlaridan foydalanishni boshqarish jarayoni umuman axborotni himoya qilish tizimida xususan axborot xavfsizligini boshqarishda muhim ahamiyatga ega.

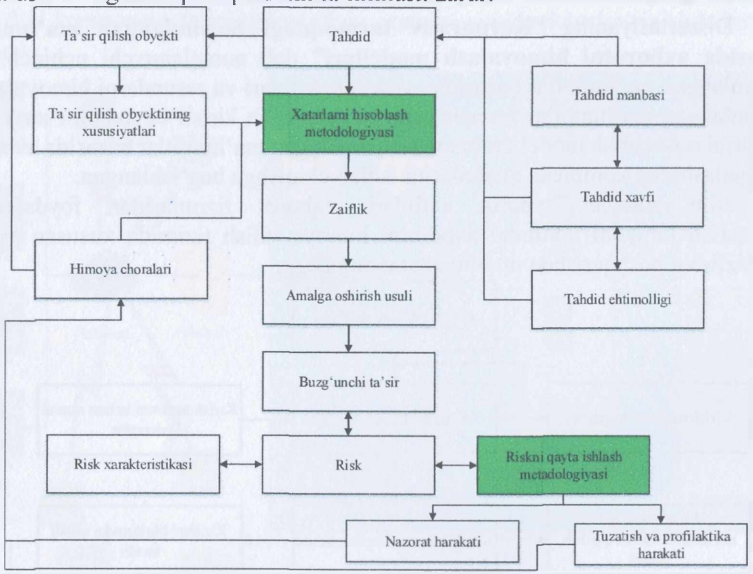


3-rasm. Himoyalangan axborot aktivlari va axborot tizimlaridan foydalanishni boshqarish jarayonida taqsimlangan ma'lumotlar bazasidagi ma'lumotlarining o'zaro ta'siri modelining umumiy sxemasi.

Ushbu jarayon tashkilotdagi taqsimlangan ma'lumotlar bazasi xavfsizligi, umumiy ma'lumotlar bazasiga bog'langan va himoya tizimi asosida himoyalangan aktivlar, axborot tizimlaridan foydalanishning to'liqligi, aniqligi, to'g'riligi va qonuniyligini ta'minlaydi, shuningdek tashkilotning ushbu tarkibiy qismlaridan va

taqsimlangan ma'lumotlar bazasida foydalanuvchilarning ruxsatsiz foydalanishni cheklash va ushbu holatga yaqin jarayonlarni sezilarli darajada qiyinlashtirishni ta'minlaydi.

Bunda taqsimlangan ma'lumotlar bazasida audit o'tkazishda audit mezonlarini tanlashga alohida e'tibor qaratish zarur. Chunki tashkilot faoliyat turi o'zgargan hollarda taqsimlangan ma'lumotlar bazasida audit o'tkazishda tanlangan mezon ustuvorligini saqlab qolishini ta'minlash zarur.

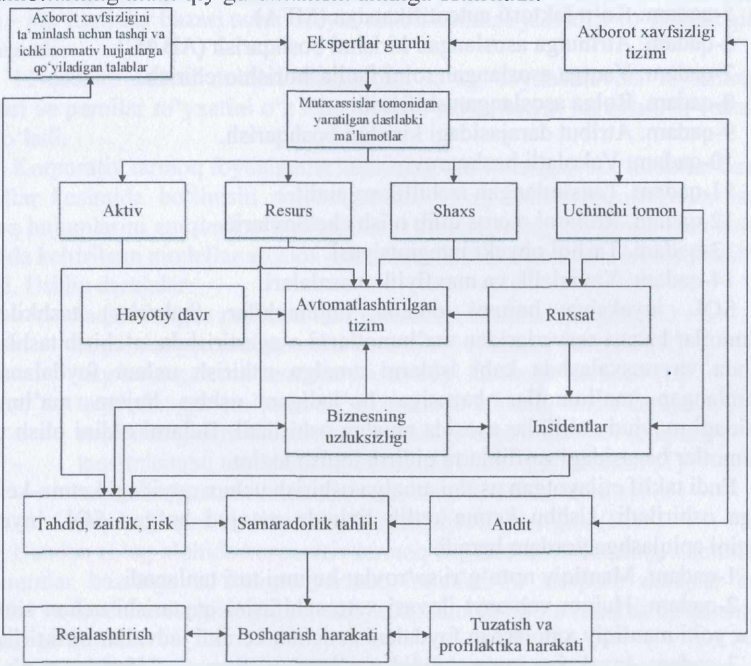


4-rasm. Axborot xavfsizligi riski va tahdidlarini boshqarish jarayonida taqsimlangan ma'lumotlar bazasidagi ma'lumotlarining o'zaro ta'siri modelining umumiy sxemasi.

Taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash va tashkilotning butun axborot tizimi doirasida axborotni himoyalash tizimi samaradorligini tahlil qilishni axborot xavfsizligini ta'minlash tizimini boshqarish jarayonining ajralmas elementi bo'lib, tashkilotda qo'llaniladigan tizim samaradorligini tahlil qilish metodologiyasini qo'llash natijalariga ko'ra shakllantiriladi hamda unga kiritilgan mos yozuvlar qiymatlariga nisbatan tashkilotning axborot xavfsizligining joriy darajasini ko'rsatadigan tahliliy hisob-kitoblarni taqdim etish uchun foydalaniladi. Bu hisob-kitoblar natijasida xavfsizlikni ta'minlashning komplek modeli ishlab chiqiladi.

Axborot xavfsizligi tizimida taqsimlangan ma'lumotlar bazasidagi ma'lumotlarning o'zaro ta'sirini jarayonli yondashuv asosida boshqarishning kompleks modelining umumiy sxemasi 5-rasmda ko'rsatilgan. Shunday qilib, ushbu modelga ko'ra, jarayon komponentlarini tavsiflashning bir qismi sifatida aniqlangan taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash va boshqarish uchun zarur bo'lgan barcha ma'lumotlar usulni qo'llash doirasida ularning funksional rolini

ta'minlaydigan guruhlarga taqsimlanadi, shundan so'ng. ular majburiy tizimlashtirishdan o'tadi va 4 ta asosiy ma'lumot blokiga (aktivlar, resurslar, xodimlar, uchinchi shaxslar) taqsimlanadi. Keyin tashkilotning tarkibiy qismlarining eng maqbul ko'rinishi axborot tizimlar doirasida tizimlashtirilgan ma'lumotlarning mantiqiy guruhlanishi amalga oshiriladi.



5-rasm. Taqsimlangan ma'lumotlar bazasidagi ma'lumotlarning o'zaro ta'sirini jarayonli yondashuv asosida boshqarishning kompleks modelining umumiy sxemasi.

Dissertasiyaning **"Taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash, zaifliklarni va tarmoq hujumlarini aniqlash usullari va algoritmlari"** deb nomlangan to'rtinchi bobi korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash hamda taqsimlangan ma'lumotlar bazasida zaifliklarni aniqlash usul va algoritmlari ishlab chiqilgan. Korxonaning ma'lumotlar bazasini tashqi va ichki tahdidlardan himoyalashni hisobga olgan holda, korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usul va algoritmi ishlab chiqilgan va boshqa turdagi hujumlardan himoyalanish tavsifiga bag'ishlangan.

Taqsimlangan ma'lumotlar bazasi muhitida ruxsatni cheklash uchun yangi algoritmni loyihalash turli omillarni, jumladan, ma'lumotlarning izchilligi, kengaytirilishi, xavfsizligi va ishlashini diqqat bilan ko'rib chiqishni talab qiladi. Quyida taqsimlangan ma'lumotlar bazasida ruxsatni cheklash algoritmi keltirilgan:

Taklif etilayotgan model algoritmi 14 qadamda tavsiflangan:

1-qadam. Rolga asoslangan kirishni boshqarish (RBAC) ishga tushirish.

2-qadam. Ma'lumotlarni ko'paytirish(replikatsiya) va sinxronlashtirish.

3-qadam. Dinamik rolni belgilash.

4-qadam. Kontekstga asoslangan kirishni boshqarish.

5-qadam. Ko'p faktorli autentifikatsiya (MFA).

6-qadam. Atributga asoslangan kirishni boshqarish (ABAC).

7-qadam. Vaqtga asoslangan rolni faollashtirish/o'chirish.

8-qadam. Rolga asoslangan shifrlash.

9-qadam. Atribut darajasidagi kirishni boshqarish.

10-qadam. Vakolatli boshqaruv.

11-qadam. Taqsimlangan izchillik va audit.

12-qadam. Rollarni meros qilib olish cheklovlari.

13-qadam. Tashqi obyekt integratsiyasi.

14-qadam. Xavfsizlik va maxfiylik masalalari.

SQL inyeksiya hujumi odatda hujumchilar (hakerlar) tashkilotning ma'lumotlar bazasi serverlaridan ma'lumotlarni o'zgartirishda, o'chirib tashlashda, o'qishda va nusxalashda kabi ishlarni amalga oshirish uchun foydalanadilar. Taqsimlangan ma'lumotlar bazasiga bo'ladigan ushbu hujum ma'lumotlar bazasidagi mavjud zaifliklar asosida amalga oshiriladi. Bularni oldini olish uchun ma'lumotlar bazasidagi zaifliklarni qidirib topish lozim.

Endi taklif etilayotgan usulni amalga oshirish uchun quyidagi ketma-ketliklar amalga oshiriladi. Ushbu ketma-ketlik tizimda mavjud bo'gan SQL inyeksiya zaifligini aniqlashga yordam beradi.

1-qadam. Mantiqiy noto'g'ri so'rovlar hujumi turi tanlanadi.

2-qadam. Hujum veb-sayt ilovasi xato sahifasini qaytarishi uchun sintaktik xatolar yoki mantiqiy xatolardan foydalanish uchun kerakli jadvallar biriktiriladi.

3-qadam. Inyeksiya login shaklidan olingan veb-sayt sahifasidan o'tib ketsa tizimda SQL inyeksiya zaifligi mavjud bo'ladi.

4-qadam. Keyingi qadamda esa foydalanilayotgan brauzerda SQL elementlarini yordamida so'rov kengyatmasini tekshirish amalga oshiriladi.

5-qadam. Ushbu elementlarni tekshirgandan so'ng, avtomatlashtirish ilovasi Python (Php...) kutubxonasidagi kutubxona so'rovlari yordamida uni qayta chaqiradi. Bunga sabab MBBT MySQL (SQL) so'rovini yuborish funksiyasi post turidir, chunki tizim ishlash prinsipi ishlab chiqilgan so'rov orqali yuborishga asoslangan.

6-qadam. Shundan so'ng funksiyada xatolikmavjud bo'lsa MBsiga kirish sahifasi orqali veb-saytga kirishga imkon beradi.

7-qadam. Ilova tomonidan yaratilgan so'rov orqali esa ma'lumotlar bazasida foydalanuvchi nomi va parolni topishga imkn beradi.

8-qadam. Inyeksiya uchta parametrdan, ya'ni ustun_nomi, birinchi_indeks va bir qator belgilardan iborat bo'lgan pastki qator () funksiyasi yordamida amalga oshiriladi.

9-qadam. Inyektsiya so‘rovi login formasidagi bo‘shliqning asosiy so‘roviga mos bo‘lib, asosiy so‘rov ishlamasligini ta’minlaydi. Bu vaqtda tizim haqiqiy inyeksiya so‘rovi bilan almashtira olmaydi.

10-qadam. Amalga oshirilgan so‘rovlar yuqoridagi yuqorida keltirilgan jadvaldagi algoritmlar bo‘yicha avtomatlashtiriladi. Izlash kerak bo‘lgan birinchi narsa – ma’lumotlar bazasi nomi. Keyin ushbu nomdan jadvallar ro‘yxatini qidirish boshlanadi.

11-qadam. Jadval nomini olingandan so‘ng, foydalanuvchi foydalanuvchi nomlari va parollar ro‘yxatini o‘z ichiga olgan jadvallardan foydalanish vakolatiga ega bo‘ladi.

Korporativ tarmoq foydalanuvchilarining taqsimlangan ma’lumotlar bazasini hududlar kesimida bo‘linishi aniqlangandan so‘ng ushbu bazalarga bo‘ladigan tarmoq hujumlarini aniqlash uchun quyidagi darajalarning har biriga mos holdatda 3-bobda keltirilgan modellar asosida juft taqqoslanishi matritsalarini hisoblash talab etiladi. Ushbu darajalar:

- taqsimlangan ma’lumotlar bazasidagi aktivlar darajasi (A)
- taqsimlangan ma’lumotlar bazasidagi resurslar darajasi (R)
- taqsimlangan ma’lumotlar bazasidagi hodimlar darajasi (H)
- taqsimlangan ma’lumotlar bazasidagi uchinchi shaxs darajasi (U)
- taqsimlangan ma’lumotlar bazasidagi hujum darajasi (Hujum)
- taqsimlangan ma’lumotlar bazasidagi tahdidlar darajasi (T)
- taqsimlangan ma’lumotlar bazasidagi zaifliklar darajasi (Z)
- taqsimlangan ma’lumotlar bazasidagi risk darajasi (Risk)

Bundan so‘ng alohida korporativ tarmoq foydalanuvchilarining taqsimlangan ma’lumotlar bazasiga bo‘ladigan tarmoq hujumlarini aniqlash darajasi hamda resurslar va foydalanuvchilar guruhi darajasida hamda bo‘limlar orasida qo‘shimcha aloqalar qo‘shiladi.

$$A = \begin{pmatrix} 1 & a_1/a_2 & \dots & a_1/a_n \\ a_2/a_1 & 1 & \dots & a_2/a_n \\ \vdots & \vdots & \dots & \vdots \\ a_n/a_1 & a_n/a_2 & \dots & 1 \end{pmatrix}, \qquad (1)$$

bu yerda A – korporativ tarmoq foydalanuvchilarining taqsimlangan ma’lumotlar bazasiga bo‘ladigan tarmoq hujumlarini aniqlashda aktivlar darajasining juft taqqoslanish matritsasi.

$$R = \begin{pmatrix} 1 & r_1/r_2 & \dots & r_1/r_k \\ r_2/r_1 & 1 & \dots & r_2/r_k \\ \vdots & \vdots & \dots & \vdots \\ r_k/r_1 & r_k/r_2 & \dots & 1 \end{pmatrix}, \qquad (2)$$

bu yerda R – korporativ tarmoq foydalanuvchilarining taqsimlangan ma’lumotlar bazasiga bo‘ladigan tarmoq hujumlarini aniqlashda resusrlar darajasining juft taqqoslanish matritsasi. Qolgan darajalar uchun ham shu tartibda hisoblashlar amalga oshiriladi va quyidagi ifoda yordamida natija aniqlanadi.

$$Natija = \begin{pmatrix} \sum_{j=1}^{n} a_j^c * \ r_i^c * h_i^c * \ u_i^c * huj_i^c * \ t_i^c * z_i^c * \ risk_1^c \\ \sum_{j=1}^{n} a_j^c * \ r_i^c * h_i^c * \ u_i^c * huj_i^c * \ t_i^c * z_i^c * \ risk_2^c \\ \sum_{j=1}^{n} a_j^c * \ r_i^c * h_i^c * \ u_i^c * huj_i^c * \ t_i^c * z_i^c * \ risk_s^c \end{pmatrix} \quad (3)$$

Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini aniqlash hamda ularni bartaraf etish korxonaning axborot xavfsizligini ta'minlash tizimi samaradorligini ortishiga yordam beradi.

Ma'lumotlar bazasiga nisbatan amalga oshirilgan hujumlarni eng katta qismini SQL inyeksiya hujumlari tashkil etgan. Shuning uchun ham ishlab chiqilgan usulni aynan shu turdagi hujumlarni aniqlash va bartaraf etish jarayonida sinovdan o'tkazilsa maqsadga muvofiq bo'ladi. Bu turdagi hujumlarni aniqlab olishda ishlab chiqilgan usul algoritmi quyidagi ketma ketlikda amalga oshiriladi. Ishlash texnologiyasi IPS algoritmiga o'xshaydi, undan asosiy farqi buyruqlar uchun vazn tushuncha kiritilgan hamda hal qiluvchi darajaga ko'ra aynan vazn tushunchasi asosida hal qilinadi. Buyruq qanchalik muhim bo'lsa, unda vazn shunchalik katta bo'ladi va shunga mos ravishda OTP (Bir martalik parol) talab qilinadi. Algoritmni ishlashi sxemasi quyida keltirilgan.

1-qadam. Boshlash.

2-qadam. Foydalanuvchi Id va Parolini olish (OTP).

3-qadam. So'rovni tahlil qilish (bunda so'rov orqali qaysi buyruq berilganligi aniqlashtirilib olinadi ya'ni Select/Insert/Delete/Update).

4-qadam. So'rov vaznini tekshirish (bunda vazn yuborilgan so'rovning chastotasiga mos holda ortib boradi, chastotasi ya'ni qanchlik tez ushbu so'rovni yuborilishlari soni kamaysa vazn tushadi).

5-qadam. Tekshirish sharti amalga oshiriladi (ya'ni shart quyidagicha: agar vazn 3 ga teng yoki undan katta bo'lsa 6-qadamga o'tish, aks holda 9-qadamga o'tish sharti bajarilsin).

6-qadam. Buyruqni yangiligini tekshiriladi.

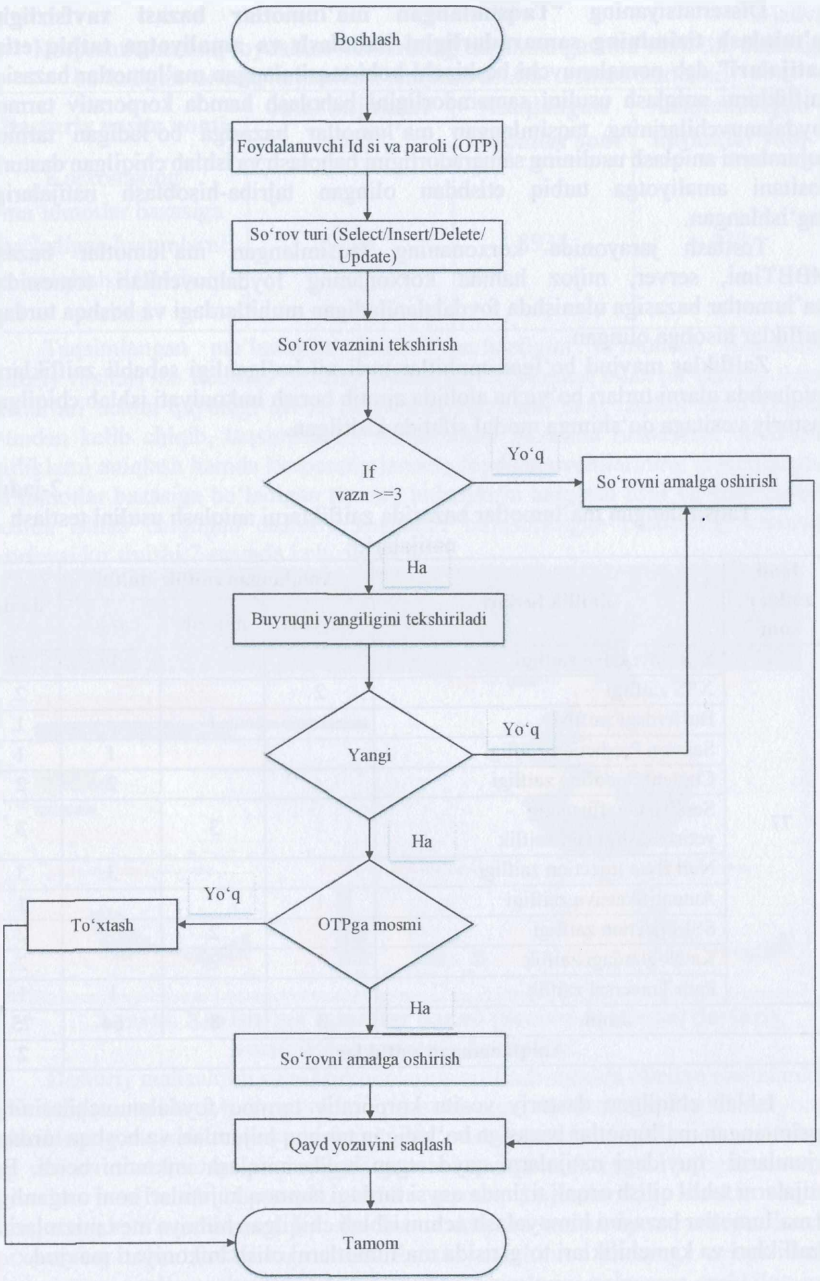
7-qadam. Quyidagi shart bo'yicha tekshirish (agar so'rov yangi bo'lsa 8-qadamga aks holda 11-qadamga o'tish shart bajarilsin).

8-qadam. Agar OTP mos bo'lsa 9 – qadamga aks holda 11-qadamga o'tish sharti bajarilsin.

9-qadam. So'rovni amalga oshirish.

10-qadam. Qayd yozuvini saqlash.

11-qadam. Tamom.



6-rasm. SQL inyeksiya hujumini aniqlsh algoritmning blok sxemasi.

Dissertatsiyaning **"Taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash tizimining samaradorligini baholash va amaliyotga tatbiq etish natijalari"** deb nomalanuvchi beshinchi bobi taqsimlangan ma'lumotlar bazasida zaifliklarni aniqlash usulini samaradorligini baholash hamda korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usulining samaradorligini baholash va ishlab chiqilgan dasturiy vositani amaliyotga tatbiq etishdan olingan tajriba-hisoblash natijalariga bag'ishlangan.

Testlash jarayonida korxonaning taqsimlangan ma'lumotlar bazasi, MBBTimi, server, mijoz hamda korxonaning foydalnuvchilari tomonidan ma'lumotlar bazasiga ulanishda foydalalaniladigan muhitlardagi va boshqa turdagi zaifliklar hisobga olingan.

Zaifliklar mavjud bo'lgan muhitlar turli xil bo'lganligi sababli zaifliklarni aniqlashda ularni turlari bo'yicha alohida ajratib berish imkoniyati ishlab chiqilgan dasturiy vositaga qo'shimga modul sifatida kiritilgan.

2-jadval

Taqsimlangan ma'lumotlar bazasida zaifliklarni aniqlash usulini testlash natijalari.

Jami zaiklar soni	Zaiflik turlari	Aniqlangan zaiflik muhiti			Jami
		serverda	mijozda	bazada	
77	SQL inyeksiya zaifligi			57	57
	XSS zaifligi	2			2
	Bufferdagi zaiflik		1		1
	Session Prediction zaifligi			1	1
	Content Spoofing zaifligi			2	2
	Sessiya tanaffusining yetishmasligidagi zaiflik		3		3
	Null Byte Injection zaifligi			3	3
	Autentifikatsiya zaifligi	1			1
	SSI Injection zaifligi		2		2
	Kataloglardagi zaiflik		2		2
	Path Traversal zaiflik			1	1
Jami		**3**	**8**	**64**	**75**
Aniqlanmagan zaifliklar					**2**

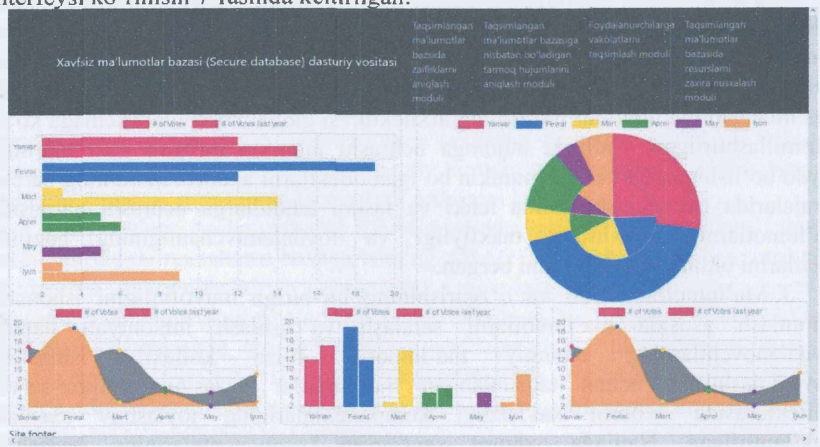
Ishlab chiqilgan dasturiy vosita korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlari va boshqa turdagi hujumlarni quyidagi natijalarni qayd etgan holda aniqlash imkonini berdi. Bu natijalarni tahlil qilish orqali tizimda qaysi turdagi taqmoq hujumlari soni ortganligi va ma'lumotlar bazasini himoyalash uchun ishlab chiqilgan himoya mexanizmlarini afzalliklari va kamchiliklari to'g'risida ma'lumotlarni olish imkoniyati mavjud.

3-jadval

Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usulini testlash natijalari.

Dasturiy vosita nomi	Jami hujumlar soni	Aniqlangan hujumlar soni	Aniqlanmagan hujumlar soni
Korxonaning ma'lumotlar bazasiga bo'ladigan hujumlarni aniqlash dasturiy vositasi	9108	8935	173

Taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash tizimining dasturiy vositasi ma'lumotlar bazasi xavfsizligini ta'minlash bilan bir qatorda tizim mamurlari uchun quyidagi qo'shimcha imkoniyatlarni ham taqdim etadi beradi. Shundan kelib chiqib, taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash, zaifliklarni aniqlash hamda korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usul va algoritmlari asosida ishlab chiqilgan dasturiy vositalari birlashtirilgan dasturning umumiy interfeysi ko'rinishi 7-rasmda keltirilgan.



7-rasm. Xavfsiz ma'lumotlar bazasi (Secure database) dasturiy vositasining umumiy ko'rinishi.

Dasturiy mahsulotni soha korxonalarida qo'llash asosida olingan natijalardan kelib chiqqan holda aytish mumkinki, taqsimlangan ma'lumotlar bazasi ixtiyoriy tashkilotning raqamli texnologiyalarni joriy etish va undan foydalanish vaqtidagi eng muhim obektlardan biri bo'lganligi sababli unga nisbatan bo'ladigan tarmoq hujumlari soni ortib bormoqda. Ushbu tarmoq hujumlaridan kerakli vaqtda himoyalanish ta'minlanmasa bir qancha moddiy va ma'naviy zararlarga hamda korxonaning obro'sizlanishiga olib kelishi mumkin. Shuning uchun ham taqsimlangan ma'lumotlar bazasini himoyalash tizimlarini qolaversa, tashkilotning

butun axborot tizimi xavfsizligini ta'minlash usullari va algoritmlarni ishlab chiqish va takomillashtirish bugunning va ertangi kunning talabi bo'lib qoladi.

XULOSA

"Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash usullari va algoritmlari" mavzusidagi dissertatsiya ishi bo'yicha olib borilgan tadqiqot natijalari asosida quyidagi xulosalar taqdim etildi:

1. Korporativ tarmoq faydalanuvchilarining taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash maqsadida, tashkilotning korporativ tarmog'ida ma'lumotlar bazasiga bo'ladigan tarmoq hujum turlari qiyosiy tahlil qilingan. Qiyosiy tahlil qilish asosida taqsimlangan ma'lumotlar bazasiga nisbatan ichki va tashqi tahdidlarni hisobga olgan holda ma'lumotlar bazasiga bo'ladigan tarmoq hujumlari 4 ta asosiy tasnifga ajratilgan. Ushbu tarmoq hujumlaridan himoyalanish tizim samaradorligini oshirish maqsadida, ularning ta'sir darajasi (yuqori, o'rta, past), ulanish rejimining onlayn va offlayn amalga oshirilishi (ulanish rejimi ichki va tashqi tarmoq turiga qarab), MBBT turiga bog'liqligi, amalga oshirish darajasi (oson, qiyin), konfidensiallikni buzishi, butunlikni buzishi va foydalanuvchanlikni buzishi kabi mezonlar asosida tahlil qilish taklif etilgan.

2. Taqsimlangan ma'lumotlar bazasi tizimlarini integratsiyalash uchun ishlab chiqilgan arxitektura (ANSI/SPARC: American National Standards Institute, Standards Planning And Requirements Committee) markazlashtirilgan MBBTlari uchun umumiy komponentga ega bo'lgan korporativ tarmoq foydalanuvchilari taqsimlangan ma'lumotlar bazasining arxitekturasi global koseptual sxemaga ko'ra takomillashtirilgan. Natijada hujumga uchrashi mumkin bo'lgan yoki ularning paydo bo'lishiga olib kelishi mumkin bo'lgan obektlarni axborot tizimining barcha darajalarida nazoratlash hamda ichki va tashqi tahdidlarga uchrashi natijasida ma'lumotlarning yaxlitligi, maxfiyligi va foydalanuvchanligining buzilish holatlarini oldini olish imkonini bergan.

3. Ma'lumotlar holati va o'zgarishining bir-biriga muvofiqligini ishonchli ta'minlash asosida ma'lumotlarni saralash va ishlash imkoniyati hamda foydalanuvchilarning umumiy ma'lumotlar bilan kollektiv ishlashini muvofiqlashtirish uchun taqsimlangan ma'lumotlar bazasining mijoz-server arxitekturasida axborot xavfsizligi komponentalarining joylashuv sxemasi shakllantirilgan. Natijada axborot xavfsizligi komponentalarining joylashuv sxemasi o'z vaqtida "mijoz-server" texnologiyalarining to'rtta modelida ma'lumotlar almashishi va komponentalarning o'zgarishini hisobga olib, tashkilotning umumiy ma'lumotlar bazasida axborotlarni foydalanuvchilarning foydalanish vakolati bo'yicha jadvallarga taqsimlash imkonini bergan.

4. Ma'lumotlar bazasidagi ma'lumotlarni to'liq, o'sib borish va differensial zaxiralash imkoniyatidan foydalangan holda real vaqt rejimida taqsimlangan ma'lumotlar bazasida resurslarni zaxira nusxalash usuli va algoritmi ishlab chiqilgan. Natijada taqsimlangan ma'lumotlar bazasi uchun qayta tiklanadigan zaxira jarayonini loyihalash va ma'lumotlarning izchilligini, xatolarga

chidamliligini va samarali tiklanishini hamda turli xil operatsion sharoitlarga moslashishini real vaqt rejimida ta'minlashga imkon bergan.

5. Qarorlarini qo'llab-quvvatlashning dinamik ekspert tizimlariga asoslangan holda foydalanish darjasiga ko'ra himoyalangan aktivlarini boshqarish va axborotni himoyalash tizimining resurslarini boshqarish jarayonida taqsimlangan ma'lumotlar bazasidagi ma'lumotlarining o'zaro ta'siri modellari ishlab chiqilgan. Natijada taqsimlangan ma'lumotlar bazasida tashkilot aktivlari va resurslarni himoyalash bo'yicha yagona himoya tizimi orqali nazoratni amalga oshirishga imkon bergan.

6. Tashkilotda foydalanilayotgan taqsimlangan ma'lumotlar bazasidagi ma'lumotlardan foydalanishni boshqarish mexanizmlaridan kelib chiqib, foydalanuvchi vakolatlarini foydalanishni boshqarish aspektlari asosida taqsimlangan ma'lumotlar bazasida ruxsat etilmagan kirish va axborot xavfsizligi risklarini boshqarish modellari takomillashtirilgan. Natijada taqsimlangan ma'lumotlar bazasiga kirishda foydalanuvchilarga tashkilot tomonidan berilgan vakolatlar doirasidan tashqari ruxsat etilmagan harakatlarini aniqlash va ushbu harakatlar asosida amalga oshiriladigan ichki va tashqi tahdidlarni aniqlash hamda axborot tizimidagi risklarni boshqarishga imkon bergan.

7. Taqsimlangan ma'lumotlar bazasi xavfsizligi va axborotni himoyalash bo'yicha ichki va tashqi huquqiy hujjatlarning talablaridan kelib chiqqan holda, umumiy resurslarning ichki va tashqi parametrlariga ko'ra ekspertlar guruhining axborotni himoya qilish tizimi va himoya qilish obektlari bo'yicha xulosasi asosida taqsimlangan ma'lumotlar bazasida axborotni himoyalashning kompleks modeli ishlab chiqilgan. Natijada taqsimlangan ma'lumotlar bazasini himoyalashda himoya mexanizmi 4 ta asosiy ma'lumot blokiga (aktivlar, resurslar, xodimlar, uchinchi shaxslar) ajratish va ular asosida korporativ tarmoqdagi tahdidlarni, zaiflikalarni va risklarni mantiqiy guruhlarga taqsimlash imkonini bergan.

8. Ruxsatlarni boshqarishning RBAC usulidagi mavjud kamchiliklarni bartaraf etish maqsadida ruxsatlarni boshqarishning ABAC usulida foydalanilgan atributlar yordamida takomillashtirish natijasida taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash usuli va algoritmi ishlab chiqilgan. Natijada foydalanuvchilarga ruxsatlarni cheklashda tizimga kirishga soddalashtirish, taqsimlangan tugunlar orasida masshtablik va moslashuvchanlikni ta'minlash, foydalanuvchilar tomonidan amalga oshiriladigan ichki va tashqi tahdidlarni oldini olish hamda ma'lumotlarning maxfiyligini ta'minlashga imkon bergan.

9. Ma'lumotlar bazasiga foydalanuvchilar tomonidan yuborilgan so'rovlarga mos javoblarni kerakli jadvallardan qidirishda chiziqli, ikkilik va interpolyatsiya qidiruv algoritmlarini qo'llash asosida axborot tizimi muhitiga ko'ra taqsimlangan ma'lumotlar bazasidagi zaifliklarni aniqlash usuli va algoritmi ishlab chiqilgan. Natijada taqsimlangan ma'lumotlar bazasidagi jadvallar taqsimlanganligi tufayli turli joylarda joylashgan bo'lishiga qaramasdan mavjud zaifliklarni axborot tizimi muhitida ya'ni server qism, mijoz qism yoki ma'lumotlar bazasi kesimida aniqlashga imkon bergan.

10. Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasida aktivlar, resurslar, xodimlar, uchinchi shaxs, hujum, tahdid, zaiflik va risk

darajalariga vazn tushunchasini kiritish asosida korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini aniqlash usuli va algoritmi takomillashtirilgan. Natijada taqsimlangan ma'lumotlar bazasiga nisbatan amalga oshiriladigan hujumlarni aniqlashga va tarmoq anomaliyalari bilan birinchi va ikkinchi turdagi xatoliklarni farqlashga imkon bergan. Korxonaning korporativ tarmog'idagi ichki va tashqi tahdidlar va tizimdagi mavjud zaifliklar asosida amalga oshirilishi mumkin bo'lgan tarmoq hujumlarini axborot tizimi muhitida bartaraf etish imkoniyati yaratilgan.

11. Taqsimlangan ma'lumotlar bazasida zaifliklarni aniqlash usuli asosida ishlab chiqilgan dasturiy vosita korxonaning taqsimlangan ma'lumotlar bazasidagi zaifliklarni 97,5 foiz aniqlik qayd etgan holda aniqlash imkonini bergan. Taqsimlangan ma'lumotlar bazasidagi jami 77 ta zaifliklarni 5 ta asosiy turga ajratgan holda aniqlash hamda ularni axborot tizimi muhitida ya'ni server muhiti, mijoz muhiti va ma'lumotlar bazasini boshqarish muhiti kesimida taqsimlash imkonini bergan.

12. Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usuli asosida ishlab chiqilgan dasturiy vosita korxonaning taqsimlangan ma'lumotlar bazasiga bo'ladigan 9108 ta tarmoq hujumlaridan 8935 tasini 98,1 foiz aniqlik qayd etgan holda aniqlash imkonini bergan. Natijada taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini nafaqat axborot tizimi (server, mijoz, baza) muhitda, qolaversa korxonaning taqsimlangan ma'lumotlar bazasining 8 ta darajasida (taqsimlangan ma'lumotlar bazasida aktivlar, resurslar, hodimlar, uchinchi shaxs, hujum, tahdid zaiflik va risk darajalari) aniqlash imkonini bergan.

13. Taqsimlangan ma'lumotlar bazasida ruxsatlarni cheklash, zaifliklarni aniqlash hamda korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarni aniqlash usul va algoritmlari asosida ishlab chiqilgan "Xavfsiz ma'lumotlar bazasi (Secure database) dasturiy vositasi" (O'zbekiston Respublikasining Dasturiy mahsulotlar davlat reyestrida 27.06.2023 y. ro'xatdan o'tkazilgan, № DGU 26031) nomli dasturiy vositaning samaradorligi boshqa dasturiy vositalarga nisbatan tarmoq hujumlarini 1,8 ms yuqori tezlikda aniqlash hamda tizimning yolg'on ishga tushish holatlari soni 1,6 marta kamaytirishga imkon bergan.

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

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАСИОННИХ ТЕХНОЛОГИЙ

САДИКОВ ШУХРАТ МУХАМАДЖАНОВИЧ

МЕТОДЫ И АЛГОРИТМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РАСПРЕДЕЛЁННОЙ БАЗЫ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ СЕТИ

05.01.05 - Методи и системи зашити информасии. Информасионная безопасность

АВТОРЕФЕРАТ ДОКТОРСКОЙ (DSc)
ДИССЕРТАСИИ ПО ТЕХНИЧЕСКИМ НАУКАМ

Ташкент – 2023

Тема докторской диссертации по техническим наукам (DSc) зарегистрирована в Высшей аттестационной комиссии при Министерство Высшего образования, науки и инноваций Республики Узбекистан за № B2023.3.DSc/T655.

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб странице (www.tuit.uz) и на Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научний консультант:	**Махкамов Бахтиёр Шухратович** доктор экономических наук, профессор
Офитсиальние оппоненти:	**Керимов Камил Фикратович** доктор технических наук, доцент
	Жураев Гайрат Умарович физико-математических наук, профессор
	Примова Холида Анарбоевна доктор технических наук, доцент
Ведушая организасия:	**Ташкентский государственный технический университет имени Ислама Каримова**

Защита диссертации состоится «21» 10 2023 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; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №284 (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-70).

Автореферат диссертации разослан «20» 10 2023 года.
(протокол рассылки №4 от «19» 10 2023 года.).

Д.Я.Иргашева
Зам. председател научного совета
по присуждению учёных степеней
доктор технических наук, профессор

Э.Ш.Назирова
Ученый секретар научного совета
по присуждению учёных степеней
доктор технических наук, профессор

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

ВВЕДЕНИЕ (Автореферат докторской диссертации (DSc))

Актуальность и востребованность темы диссертации. В условиях современного состояния и перспектив развития мировой экономики на приоритетном уровне, основанном на цифровых технологиях и технологиях искусственного интеллекта, одной из важнейших проблем остается эффективная защита предприятий от киберугроз и кибератак при эффективном обеспечении систем управления приемом, обработкой, хранением и передачей информации. Согласно статистике Kaspersky, количество атак на базы данных составило 27% от всех атак в 2020 году, в то время как за последние три года этот показатель увеличился в 2,8 раза и составил 75,6% от общего числа кибератак в 2023 году[1]. При создании эффективной системы защиты информационных систем от киберугроз и кибератак в современном мире особое внимание уделяется таким мерам, как организация программно-технологического обеспечения надежной защиты баз данных предприятия, составляющих основу создания информации, повышение эффективности системы защиты распределённых баз данных, надежная защита пользователей корпоративных сетей от сетевых атак в распределённых базах данных, применение эффективных методов и алгоритмов обнаружения угроз.

Во всем мире на приоритетном уровне реализуются исследовательские проекты, направленные на разработку архитектуры распределённых баз данных корпоративных сетевых пользователей предприятий, методов и алгоритмов резервного копирования ресурсов в распределённых базах данных, а также методов и алгоритмов ограничения разрешений в распределённых базах данных. В связи с этим особое внимание уделяется исследованиям по таким темам, как защита активов и ресурсов организации в распределённых базах данных, управление рисками несанкционированного доступа и информационной безопасности, а также разработка комплексных моделей защиты информации в распределённых базах данных, разработка методов и алгоритмов обнаружения уязвимостей в распределённых базах данных и сетевых атак пользователей корпоративных сетей на распределённые базы данных.

В процессе построения Нового Узбекистана одним из приоритетов стратегического развития страны определена цифровизация экономики, в рамках стратегии "цифровой Узбекистан–2030" необходимо вывести сферу информационно-коммуникационных технологий на качественно новый уровень, контролировать внедрение информационных технологий и коммуникаций, осуществляются комплексные программные мероприятия по совершенствованию системы их защиты и укреплению организационных и программно-технологических основ в соответствии с современными

[1] https://securelist.ru/it-threat-evolution-q1-2023-pc-statistics/107526/
https://securelist.ru/it-threat-evolution-q1-2023/107467/
https://securelist.ru/it-threat-evolution-q1-2023-mobile-statistics/107514/

требованиями.[2] Для эффективной организации выполнения данных задач целесообразно углубить исследования в таких областях, как защита активов и ресурсов организации в распределённых базах данных, управление рисками несанкционированного доступа и информационной безопасности, а также разработка комплексных моделей защиты информации в распределённых базах данных, эффективное выявление уязвимостей и сетевых атак пользователей корпоративных сетей на распределённые базы данных.

Указ Президента Республики Узбекистан от 28 января 2022 года № УП-60 «О стратегии развития Нового Узбекистана на 2022 — 2026 годы», Постановление Президента Республики Узбекистан от 22 августа 2022 года № ПП-357 «О мерах по поднятию на новый уровень сферы информационно-коммуникационных технологий в 2022-2023 годах», Указ Президента Республики Узбекистан от 19 февраля 2018 года № УП-5349 «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», Постановление Президента Республики Узбекистан от 21 ноября 2018 года № ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты», Постановление Президента Республики Узбекистан от 14 сентября 2019 года № ПП-4452 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» а также, данное диссертационное исследование в определенной степени служит для реализации задач, определенных в других нормативных правовых документах, связанных с данной деятельностью.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в рамках приоритетного направления Развитии науки и технологий IV. «Информатизация и развитие информационно-коммуникационных технологий».

Обзор научных исследований по теме диссертации[3]. Научные исследования, направленные на разработку методов и алгоритмов обеспечения безопасности распределённых баз данных пользователей корпоративной сети, проводятся в ведущих научно-исследовательских институтах мира, научно-исследовательских центрах и высших учебных заведениях, в том числе в Санкт-Петербургском политехническом университете им. Петра Великого и Московском государственном техническом университете им. Н.Е.Баумана (Россия), университете Донгук (Южная Корея), Гонконгском университете науки и технологий (Китай), Швейцарском федеральном технологическом институте (Швейцария), Массачусетском Технологическом Институте (США), Южнокорейском научно-исследовательском институте науки и технологий (Южная Корея),

[2] Указ Президента Республики Узбекистан, от 28.01.2022 г. № УП-60.

[3] Обзор научных исследований по теме диссертации составлен на основании https://www.researchgate.net, www.elsevier.com. http://www.machinelearning.ru, http://www.bmstu.ru, https://habr.com и других источников

Токийском технологическом институте (Япония), Мюнхенском техническом университете (Германия), Делфтском технологическом университете (Нидерланды), Китайском университете науки и технологий (Китай) и в нашей республике Ташкентском университете информационных технологий имени Мухаммада ал-Хоразмий, Национальом университете Узбекистана имени Мирзо Улугбека, Научно-исследовательском институте развития цифровых технологий и искусственного интеллекта, в Государственном унитарном предприятии «Центр кибербезопасности», а также в Государственном унитарном предприятии «UNICON.UZ» - центр научно-технических и маркетинговых исследований (Республика Узбекистан).

Получены следующие научные результаты в мире по защите активов и ресурсов организации в распределённых базах данных, управлению рисками несанкционированного доступа и информационной безопасности, а также по разработке комплексных моделей защиты информации в распределённых базах данных, в том числе: архитектура распределённых баз данных пользователей корпоративной сети, разработаны методы резервного копирования ресурсов в распределённых базах данных (Швейцарский федеральный технологический институт (Швейцария), Массачусетский технологический институт (США)), разработаны алгоритмы ограничения разрешений на распределённую базу данных (Университет Донгук (Южная Корея), Делфтский технологический университет (Нидерланды)), разработаны методы и алгоритмы обнаружения сетевых атак на распределённую базу данных пользователей корпоративных сетей (Массачусетский технологический институт (США), Н.Е.Московский государственный технический университет им. Баумана (Россия)).

В мире ведутся исследования на приоритетном уровне по совершенствованию и разработке методов и алгоритмов обеспечения безопасности распределённых баз данных пользователей корпоративных сетей, в том числе по следующим направлениям: Архитектура распределённых баз данных пользователей корпоративных сетей, совершенствование методов и алгоритмов резервного копирования ресурсов в распределённых базах данных с учетом режима реального времени; разработка метода и алгоритма ограничения разрешений в распределённой базе данных в соответствии с компетенциями пользователей; защита активов и ресурсов организации в распределённой базе данных, управление рисками несанкционированного доступа и информационной безопасности, а также разработка комплексных моделей защиты информации в распределённой базе данных с учетом активов и ресурсов в корпоративной сети организации; совершенствование методов и алгоритмов обнаружения системных уязвимостей и сетевых атак на распределённую базу данных пользователей корпоративной сети на основе разделения по уровням.

Степен изученности проблемы. Ведутся научные исследования зарубежными учёными М.Малик, Т.Пател, И.Гафир, Ж.Салим, М. Хаммоудех, П.К.Паул, П.С. Аитхал, С. Б. Садкхан и другими учёными по внедрению новых

методов и алгоритмов современных механизмов защиты на основе дискретной математики, теории графов, моделирования случайных процессов, моделей на основе машинного обучения и аналогичных интеллектуальных методов в защите распределённых баз данных пользователей корпоративных сетей. Применяя современные методы защиты активов и ресурсов организации в распределённой базе данных, управления рисками несанкционированного доступа и информационной безопасности, а также разработки комплексных моделей защиты информации в распределённой базе данных научные исследования проводились такими учёными, как А. Сувалка, С. Кумар, Дж. С. Огбонна, Ф. О. Нвокома, Х.Ван, Л.Чжоу, Юань, В. Шарма, В. Ли. Следует отметить, что в настоящее время, научные школы данных учёных, продолжают свои исследования. Кроме того, организациями InfoWatch, Ideco, Cyberbit, Juniper Networks, Fortinet, Garda Technologies и Cloud Networks проводятся научно-практические инженерные исследования, направленные на обеспечение безопасности распределённых баз данных, а также на разработку программно-аппаратных средств защиты информации во всей информационной системе предприятия.

В Узбекистане научными коллективами под руководством Т.Ф.Бекмуратова, С.К.Ганиева, М.М.Каримова, И.Я.Иргашевой, Н.А.Игнатьева, Г.Жураева, Р.Х.Хамдамова, К. Керимова проведены научные исследования по выявлению уязвимостей в распределённых базах данных пользователей корпоративных сетей и разработке методов и алгоритмов обнаружения сетевых атак на распределённые базы данных пользователей корпоративных сетей.

В то же время защита активов и ресурсов организации в распределённых базах данных, управление рисками несанкционированного доступа и информационной безопасности, а также разработка комплексных моделей защиты информации в распределённых базах данных и архитектура распределённых баз данных пользователей корпоративной сети, совершенствование методов и алгоритмов резервного копирования ресурсов в распределённых базах данных.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках проекта по темам 598661-EPP-12018-1-RO-EPPKA2-CBHE-JP «Developing Services for Individuals with Disabilities» и «Теоретические методологические основы создания интеллектуальных программно-технических систем цифровой обработки сигналов и изображений на фрагментарно-полиномиальных основаниях» плана научно-исследовательской работы Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий.

Целью исследования является разработка эффективных методов и алгоритмов обнаружения уязвимостей и сетевых атак в распределённой базе

данных пользователей корпоративной сети, позволяющих повысить эффективность системы защиты распределённых баз данных.

Задачи исследования:

сравнительный анализ типов сетевых атак на базу данных в корпоративной сети и их классификация;

разработка архитектуры распределённой базы данных пользователей корпоративной сети;

разработка метода и алгоритма резервного копирования ресурсов в распределённой базе данных;

разработка моделей защиты активов и ресурсов организации и управления рисками несанкционированного доступа и информационной безопасности в распределённой базе данных;

разработка комплексной модели защиты информации в распределённой базе данных;

разработка метода и алгоритма ограничения разрешений в распределённой базе данных;

разработка метода и алгоритма обнаружения уязвимостей в распределённой базе данных;

разработка метода и алгоритма обнаружения разделенных сетевых атак на распределённую базу данных пользователей корпоративной сети.

Объектом исследования является процесс защиты распределённой базы данных пользователей корпоративных сетей Республики Узбекистан.

Предметом исследования являются методы и алгоритмы выявления и устранения уязвимостей и сетевых атак в распределённой базе данных пользователей корпоративной сети.

Методы исследования. В ходе исследования были использованы теория вероятностей, теория множеств, дискретная математика, теория моделирования случайных процессов, методы защиты баз данных, методы объектно-ориентированного программирования и другие методы.

Научная новизна исследования заключается в следующем:

усовершенствована архитектура, разработанная для интеграции систем распределённых баз данных (ANSI/SPARC: American National Standards Institute, Standards Planning And Requirements Committee) корпоративные сетевые пользователи с общим компонентом для централизованных СУБД архитектура распределённых баз данных в соответствии с глобальной концептуальной схемой;

разработан метод и алгоритм резервного копирования ресурсов в распределённой базе данных с использованием возможности полного, инкрементального и дифференциального резервного копирования данных в базе данных;

разработаны модели взаимодействия ее информации в распределённой базе данных на основе динамических экспертных систем поддержки принятия решений по управлению защищенными активами и управления ресурсами системы защиты информации;

усовершенствованы модели управления рисками несанкционированного доступа и информационной безопасности в распределённой базе данных исходя из механизмов управления использованием данных в распределённой базе данных, используемых в организации, на основе аспектов управления использованием полномочий пользователей;

разработана комплексная модель защиты информации в распределённой базе данных исходя из требований внутренних и внешних правовых актов по безопасности и защите информации распределённой базы данных, на основании заключения экспертной группы по внутренним и внешним параметрам общих ресурсов по системе защиты информации и объектам защиты;

разработан метод и алгоритм обнаружения уязвимостей в распределённой базе данных, основанный на использовании алгоритмов линейного, бинарного и интерполяционного поиска при выборе в таблицах соответствующих ответов на запросы, направляемые пользователями в базу данных;

усовершенствован метод и алгоритм обнаружения разделенных сетевых атак на распределённую базу данных пользователей корпоративной сети на основе введения понятия вес активов на ресурсы, персонала, третьей стороны, атак, угроз, уязвимостей и уровней риска в распределённой базе данных пользователей корпоративной сети.

Практические результаты исследования заключаются в следующем:

разработаны метод и алгоритм ограничения разрешений в распределённой базе данных в результате доработки существующих недостатков метода управления разрешениями RBAC с помощью атрибутов метода управления разрешениями ABAC;

разработан программный инструмент резервного копирования и обеспечения безопасности ресурсов с использованием схемы размещения компонентов информационной безопасности в клиент-серверной архитектуре распределенной базы данных;

разработано программное средство для определения полномочий пользователей и распределения ролей с использованием разработанного метода и алгоритма в результате улучшения существующих недостатков метода управления разрешениями RBAC с помощью атрибутов метода управления разрешениями ABAC;

разработано программное средство для выявления уязвимостей в распределённой базе данных с использованием разработанного метода и алгоритма с применением алгоритмов линейного, двоичного и интерполяционного поиска при поиске в требуемых таблицах соответствующих ответов на запросы пользователей к базе данных;

разработано программное средство для обнаружения возможных сетевых атак по отношению к распределённой базе данных с использованием разработанного метода и алгоритма путем введения понятия веса активов,

ресурсов, персонала, третьей стороны, атак, угроз, уязвимостей и уровней риска в распределённой базе данных пользователей корпоративной сети.

Достоверности результатов исследования. Целесообразность применяемых в исследовании подходов и методов объясняется тем, что данные получены из официальных источников, в том числе из статистических данных государственного унитарного предприятия Центр кибербезопасности и Министерства цифровых технологий Республики Узбекистан, а соответствующие выводы и предложения внедрены в практику ответственными организациями.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования заключается в том, что распределённая архитектура баз данных пользователей корпоративной сети, методы и алгоритмы резервного копирования ресурсов в распределённой базе данных в соответствии с уровнем использования в реальном времени, ограничение разрешений в распределённой базе данных в частности, служит для разработки и совершенствования методов и алгоритмов обнаружения уязвимостей в распределённой базе данных и сетевых атак пользователей корпоративной сети на распределённую базу данных, а также для разработки систем защиты информации в корпоративной сети организации.

Практическая значимость результатов исследования заключается в том, что с помощью программного обеспечения, разработанного на основе предложенных методов и алгоритмов, организация может по роду деятельности определять уязвимости в распределённой базе данных пользователей корпоративной сети и обнаруживать сетевые атаки на базу данных и способствовать автоматизации системы обеспечения информационной безопасности во всей информационной системе предприятия, а также применять полученные результаты для выявления уязвимостей в объекте защиты на уровне среды (сервера, клиента, база) наряду с определением, это объясняется тем, что позволяет сократить и эффективно использовать ресурсы организации, расходуемые на защиту базы данных от сетевых атак.

Внедрение результатов исследования. На основе научных результатов, полученных по методам и программным средствам обеспечения безопасности распределенных баз данных пользователей корпоративной сети:

разработано программное средство для интеграции систем распределённых баз данных (ANSI/SPARC: American National Standards Institute, Standards Planning and Requirements Committee) на архитектуре распределённых баз данных пользователей корпоративных сетей с общим компонентом для централизованных СУБД, внедрен в практическую деятельность ГУП "Центр кибербезопасности" (Справка Министерства цифровых технологий № 33-8 / 5665 от 18 августа 2023 года). Научное исследование показало, что программный инструмент, разработанный на основе метода обнаружения уязвимостей в распределённой базе данных,

позволил выявить 77 уязвимостей 5 основных типов в распределённой базе данных предприятия с точностью 97,5%;

программное средство, разработанный на основе метода и алгоритма резервного копирования ресурсов в распределённой базе данных в режиме реального времени с использованием возможности полного, инкрементального и дифференциального резервного копирования данных в базе данных, внедрен в практическую деятельность ГУП "Центр кибербезопасности" (Справка Министерства цифровых технологий № 33-8/5665 от 18 августа 2023 года). Научное исследование позволило выявить 8935 из 9108 возможных сетевых атак на распределённую базу данных предприятия с точностью 98,1 процента. Сравнение с применяемыми программными средствами с целью определения эффективности данного программного средства показало, что по сравнению с другими программными средствами скорость обнаружения сетевых атак на 1,8 микросекунд выше, а количество случаев ложного запуска системы в 1,6 раза меньше.

программное средство, разработанное на основе моделей взаимодействия информации в распределённой базе данных в процессе управления ресурсами системы управления и защиты информации, защищенных по уровню использования, на основе динамических экспертных систем поддержки принятия решений внедрен в практическую деятельность общества с ограниченной ответственностью «Единый интегратор по созданию и поддержке государственных информационных систем "UZINFOCOM" (справочник Министерства цифровых технологий № 33-8/5665 от 18 августа 2023 года). Научное исследование позволило выявить 76 уязвимостей 6 основных типов в распределённой базе данных предприятия с точностью 98,2%, а также выявить 7560 из 7683 сетевых атак на распределённую базу данных предприятия с точностью 98,3%;

программное средство, разработанное на основе моделей управления рисками несанкционированного доступа и информационной безопасности в распределённой базе данных на основе аспектов управления использованием полномочий пользователей, исходя из используемых в организации механизмов управления использованием информации в распределённой базе данных, внедрен в практическую деятельность общества с ограниченной ответственностью "Единый интегратор по созданию и поддержке государственных информационных систем "UZINFOCOM" (Справка Министерства цифровых технологий №33-8/5665 от 18 августа 2023 года). Сравнение с применяемыми программными средствами с целью определения эффективности данного программного средства показало, что по сравнению с другими программными средствами скорость обнаружения сетевых атак на 2,1 микросекунд выше, а количество случаев ложного запуска системы в 1,7 раза меньше;

программное средство, разработанный на основе комплексной модели защиты информации в распределённой базе данных на основе заключения экспертной группы по системе защиты информации и объектам защиты по

внутренним и внешним параметрам общих ресурсов, исходя из требований внутренних и внешних правовых актов по безопасности и защите информации внедрен в практическую деятельность ГУП "Центр электромагнитной совместимости" – "ЦЭМС" (Справка Министерства цифровых технологий № 33-8/5665 от 18 августа 2023 года). Научное исследование позволило выявить 84 уязвимости 6 основных типов в распределённой базе данных предприятия с точностью 97,1%, а также выявить 6417 из 6574 сетевых атак на распределённую базу данных предприятия с точностью 97,6%;

программное средство, разработанное на основе метода и алгоритма обнаружения уязвимостей в базе данных, распределённых по средам информационной системы, на основе применения линейных, двоичных и интерполяционных алгоритмов поиска в нужных таблицах соответствующих ответов на запросы пользователей к базе данных, внедрен в практическую деятельность "Центра электромагнитной совместимости" - ГУП "ЦЭМС" (Справка Министерства цифровых технологий № 33-8/5665 от 18 августа 2023 года). Сравнение с существующими программными средствами с целью определения эффективности данного программного средства показало, что по сравнению с другими программными средствами скорость обнаружения сетевых атак на 1,65 микросекунд выше, а количество случаев ложной активации системы в 1,33 раза меньше;

программное средство, разработанное на основе метода и алгоритма обнаружения сетевых атак пользователей корпоративной сети на распределённую базу данных, основанный на введении понятия веса активов, ресурсов, персонала, третьей стороны, атак, угроз, уязвимостей и уровней риска в распределённой базе данных пользователей корпоративной сети внедрен в практическую деятельность ГУП "Центр радиосвязи, радиовещания и телевидения" – "ЦРРТ" (Справка Министерства цифровых технологий № 33-8/5665 от 18 августа 2023 года). Научное исследование позволило выявить 52 уязвимости 4 основных типов в распределённой базе данных с точностью 97,8%, а также выявить 5304 из 5462 сетевых атак на распределённую базу данных предприятия с точностью 97,1%. Для определения эффективности данного программного средства в результате сравнения с существующими программными средствами было установлено, что скорость обнаружения сетевых атак на 1,9 микросекунд выше, а количество случаев ложной активации системы в 1,8 раза меньше.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 5 международных и 7 республиканских научно-практических конференциях.

Опубликованность результатов исследования. Всего по теме диссертации опубликовано 28 научных работ, в том числе 13 статей в научных изданиях Высшей аттестационной комиссии Республики Узбекистан, рекомендованных к публикации основных научных результатов диссертаций, из них 6 опубликовано в зарубежных и 7 в республиканских журналах, получены 3 свидетельства на регистрацию программных средств ЭВМ.

Структура и объём диссертации. Диссертация состоит из введения, пяти глав, заключения, списка использованной литературы и приложений. Объем диссертации – 191 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность темы диссертации, представлен краткий анализ проблем безопасности распределенных баз данных, определены цели и задачи исследования. Описывается научная новизна и указывается практическая значимость результатов работы, приводятся основные научные обстоятельства, подлежащие защите, приводятся сведения о внедрении результатов исследования, публикации результатов и структуре диссертации.

В первой главе диссертации, под названием **«Исследование распределенных систем защиты баз данных в корпоративной сети»**, рассматриваются типы сетевых атак на базу данных в корпоративной сети и их классификация, а также доступ к распределенной базе данных на основе несанкционированных действий, а также случаи нарушения безопасности базы данных и сравнительный анализ моделей безопасности, используемых для их защиты, а также количественная оценка целостности и анализ получения информации, предоставляется обратная связь о снижении частоты поломок в системах обработки и передачи.

Таблица 1.

Сравнительный анализ возможных сетевых атак на базу данных

Название атаки / Критерия	Атака инъекции SQL	Атака нестандартного протокола	Атака Ping Flooding	Атаки фрагментации данных
Уровень влияния (высокий, средний, низкий)	высокий	низкий	средний	низкий
Онлайн и Офлайн (по виду внутренней и внешний сети режима подключения)	Онлайн и офлайн	Онлайн	Онлайн	Онлайн
Зависимость вида СУБД	Зависимый	Зависимый	Зависимый	Зависимый
Уровень реализации (легко, трудно)	Легко	Трудно	Легко	Трудно
Нарушения конфиденциальности	+	+	-	+
Нарушения целостности	+	+	-	+
Нарушения доступности	+	-	+	+

Модели безопасности баз данных играют важную роль в обеспечении безопасности баз данных. Одним из основных направлений обеспечения информационной безопасности является определение ролей пользователей базы данных и контроль правильности использования ими предоставленных им полномочий исходя из ролей, а также при необходимости ограничение их использования. Сегодня используются следующие модели безопасности:

Дискретная модель Харрисона-Руццо Ульмана. Модель Гогера-Гезингера.Модель Беллы-Ла Падулы. Модель Биба. Модель Кларка Уилсона. Модель Миллена. Модель Сазерленда. Ролевая модель безопасности.

Потеря данных (нарушение их целостности) может наблюдаться на любом этапе сбора, регистрации, контроля, обработки, передачи данных по каналам связи в распределенной базе данных. Для предотвращения потери данных при хранении принимаются специальные меры по защите носителей информации от механических повреждений и физических воздействий (например, магнитных полей).

Поэтому выявленные угрозы и уязвимости распределенной базы данных в связи с многоуровневой архитектурой распределенной базы данных, новыми технологиями обработки информации и новыми требованиями к форме представления данных должны быть устранены.

Во второй главе диссертации, под названием **«Метод и алгоритм резервного копирования ресурсов и компонентов информационной безопасности в распределенной базе данных»**, представлены отзывы пользователей корпоративных сетей о разработке архитектуры распределенной базы данных и схемы расположения компонентов информационной безопасности в архитектуре клиент-сервер распределенной базы данных, а также предложения по повышению эффективности системы защиты распределенной базы данных и посвящена разработке метода и алгоритма резервного копирования ресурсов в распределенной базе данных.

Разделение пользователей корпоративной сети на группы с распределением базы данных, которую они используют при обеспечении безопасности базы данных, и предоставление им права использовать информацию в этих группах на основе полномочий, предоставленных пользователями в зависимости от их ролей, приведет к повышению эффективности системы обеспечения безопасности базы данных.

В современных операционных системах количество различных типов защищаемых объектов может достичь нескольких десятков, а количество различных типов, защищаемых информационных потоков-нескольких сотен. Следовательно, возможность реализации любая атака, выполняемая в операционной системе, во многом определяется архитектурой и конфигурацией операционной системы. При его разработке использовалась архитектура, специально разработанная ANSI/SPARC (американский Национальный институт стандартов, комитет по планированию и требованиям стандартов) для систем распределенных баз данных. Архитектура распределенной базы данных пользователей предлагаемой корпоративной сети представлена на рисунке 1.

Для обеспечения безопасности распределенной базы данных большое значение имеет расположение компонентов информационной безопасности в архитектуре клиент-сервер. Основной причиной этого являются пользователи, и в процессе получения необходимой им информации из базы данных компании, они наделяются полномочиями, но не все пользователи используют

свои полномочия по назначению. Поэтому необходимо постоянно следить за ситуациями использования системы пользователями и разрабатывать механизмы реагирования на них в момент обнаружения несанкционированных действий.

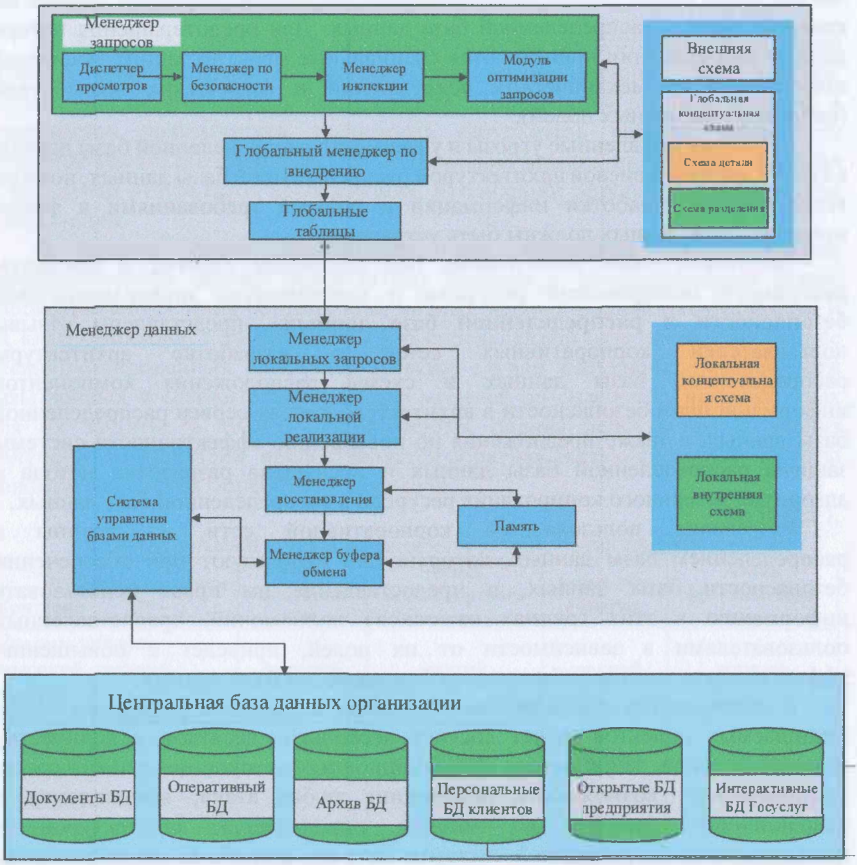


Рисунок 1. Архитектура распределенной базы данных пользователей корпоративной сети.

Исходя из этого, схема расположения компонентов информационной безопасности в клиент-серверной архитектуре распределенной базы данных выглядит следующим образом (Рис.2.).

В современную эпоху приложений и систем, основанных на данных, эффективное управление и защита данных стало приоритетом. Распределенные базы данных широко распространены из-за своей масштабности и преимуществом в производительности. Алгоритм резервного копирования ресурсов в распределенной базе данных:

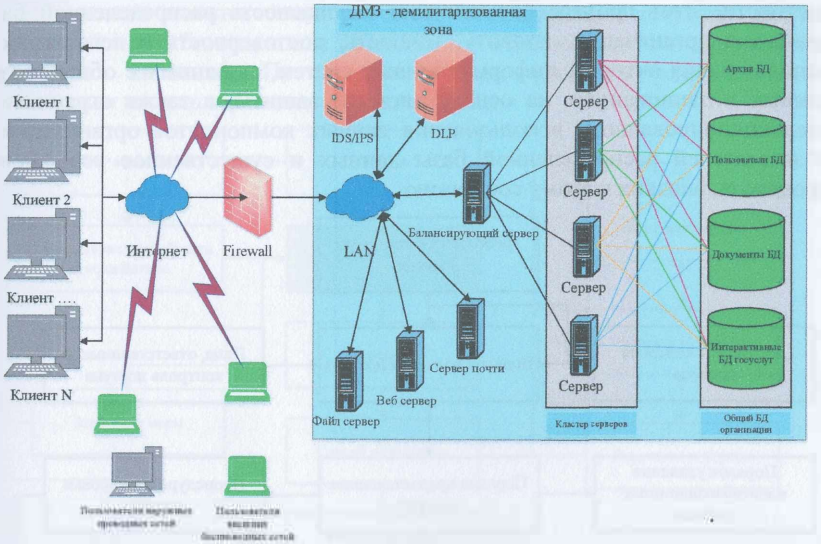


Рисунок 2. Схема расположения компонентов информационной безопасности в клиент-серверной архитектуре распределенной базы данных.

Шаг 1. Запуск процесса резервного копирования.

Шаг 2. Резерв на уровне подразделения.

Шаг 3. Распределение и потоковая передача данных.

Шаг 4. Внедрение эффективных механизмов передачи данных с учетом сжатия и шифрования.

Шаг 5. Обратимые контрольные точки.

Шаг 6. Обработка и восстановление ошибок.

Шаг 7. Функция приостановки и возобновления.

Шаг 8. Продолжение с контрольно-пропускных пунктов.

Шаг 9. Заполнение и проверка.

Шаг 10. Резервное копирование и каталогизация метаданных.

Шаг 11. Отчетность и мониторинг резервного копирования.

Шаг 12. Хранение и управление.

Шаг 13. Тестирование и проверка.

Третья глава диссертации, под названием **«Модели защиты информации в распределенной базе данных в корпоративной сети»**, посвящена описанию моделей защиты активов и ресурсов организации в распределенной базе данных и управления рисками несанкционированного доступа и информационной безопасности в распределенной базе данных, а также разработке комплексных моделей защиты информации в распределенной базе данных.

Процесс управления использованием защищенных информационных активов, информационных систем имеет важное значение в системе защиты информации в целом, и в управлении информационной безопасностью, в

частности. Этот процесс обеспечивает безопасность распределенной базы данных в организации, полноту, точность, достоверность и легитимность использования активов, информационных систем, связанных с общей базой данных и защищенных на основе системы защиты, а также ограничение несанкционированного использования данных компонентов организации и пользователей распределенной базы данных и существенное усложнение процессов, близких к этому состоянию.

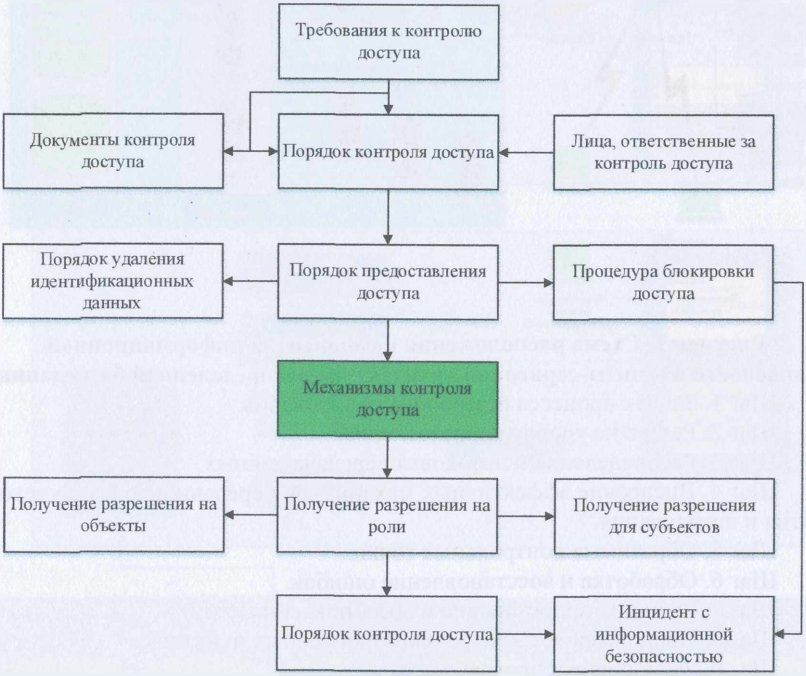


Рисунок 3. Общая схема модели взаимодействия защищенных информационных активов и их информации в распределенной базе данных в процессе управления использованием информационных систем.

При этом при проведении аудита в распределенной базе данных необходимо уделять особое внимание выбору критериев аудита. Потому что необходимо обеспечить, чтобы организация сохраняла приоритет выбранного критерия при проведении аудита распределенной базы данных в случае изменения вида деятельности.

Распределенная база данных является составным элементом процесса управления информационной безопасностью и анализа эффективности системы защиты информации в рамках всей информационной системы организации, формируется по результатам применения применяемой в организации методологии анализа эффективности системы и используется для

предоставления аналитических расчетов, показывающих текущий уровень информационной безопасности организации относительно входящих в нее справочных значений. По результату этих расчетов разрабатывается комплексная модель обеспечения безопасности.

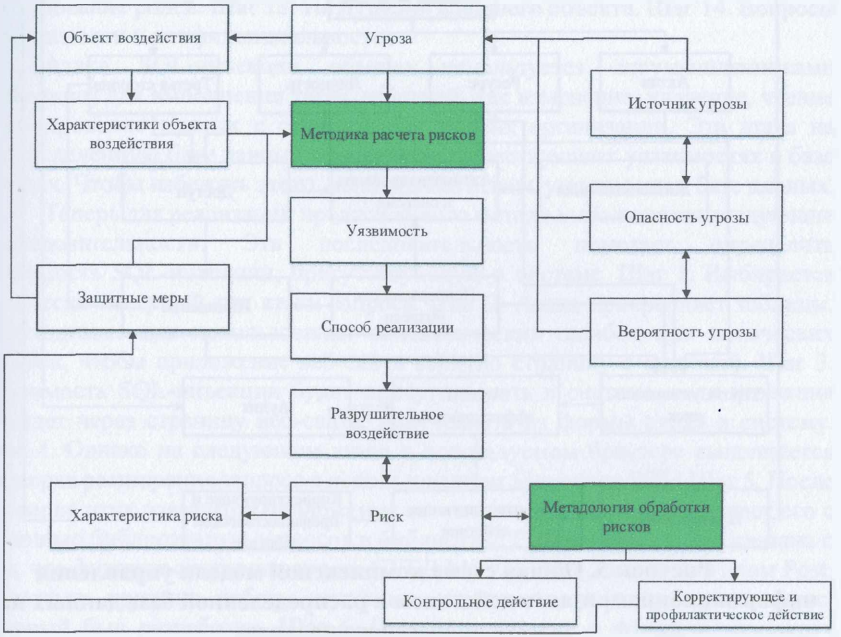


Рисунок 4. Общая схема модели взаимодействия рисков и угроз информационной безопасности в распределенной базе данных в процессе управления.

Общая схема комплексной модели управления информационным взаимодействием в распределенной базе данных в системе информационной безопасности на основе процессного подхода показана на рисунке 5. Таким образом, согласно этой модели, вся информация, необходимая для обеспечения безопасности и управления распределенной базой данных, определяемая как часть описания компонентов процесса, распределяется по группам, которые обеспечивают их функциональную роль в рамках применения метода, после чего. они проходят обязательную систематизацию и распределяются по 4 основным информационным блокам (активы, ресурсы, персонал, третьи лица). Затем осуществляется логическая группировка систематизированной информации в рамках информационных систем оптимального представления компонентов организации.

Рисунок 5. Общая схема комплексной модели управления информационным взаимодействием в распределенной базе данных на основе процессного подхода

В четвертой главе диссертации, озаглавленной **«Методы и алгоритмы обнаружения уязвимостей и сетевых атак, ограничение разрешений в распределенной базе данных»**, разработаны методы и алгоритмы ограничения разрешений в распределенной базе данных пользователей корпоративной сети, а также выявления уязвимостей в распределенной базе данных. С учетом защиты базы данных предприятия от внешних и внутренних угроз разработан метод и алгоритм обнаружения разделяемых сетевых атак на распределенную базу данных пользователей корпоративной сети и посвящен описанию защиты от других видов атак.

Разработка нового алгоритма для ограничения разрешений в среде распределенной базы данных требует тщательного рассмотрения различных факторов, включая согласованность, масштабируемость, безопасность и производительность данных. Ниже приведен алгоритм ограничения разрешений в распределенной базе данных: Алгоритм предлагаемой модели описан в 14 шагах: Шаг 1. Управление доступом на основе ролей (RBAC) запуск. Шаг 2. Воспроизведение (репликация) и синхронизация данных. Шаг 3. Определение динамической роли. Шаг 4. Контекстно-зависимый контроль доступа. Шаг 5. Многофакторная аутентификация (MFA). Шаг 6. Контроль

доступа на основе атрибутов (ABAC). Шаг 7. Активация/деактивация ролей в зависимости от времени. Шаг 8. Ролевое шифрование. Шаг 9. Контроль доступа на уровне атрибутов. Шаг 10. Грамотное управление. Шаг 11. Распределенная согласованность и аудит. Шаг 12. Ограничения на наследование ролей. Шаг 13. Интеграция внешнего объекта. Шаг 14. Вопросы безопасности и конфиденциальности.

Атака SQL-инъекции обычно используется злоумышленниками (хакерами) для выполнения таких действий, как изменение, удаление, чтение и копирование данных с серверов баз данных организации. Эта атака на распределенную базу данных основана на существующих уязвимостях в базе данных. Чтобы избежать этого, необходимо искать уязвимости в базе данных.

Теперь для реализации предложенного метода выполняются следующие последовательности. Эта последовательность помогает определить уязвимость SQL-инъекции, присутствующую в системе. Шаг 1. Выбирается логически неверный тип атаки запроса. Шаг 2. Атака прикрепляет таблицы, необходимые для использования синтаксических ошибок или логических ошибок, чтобы приложение веб-сайта вернуло страницу с ошибкой. Шаг 3. Уязвимость SQL-инъекции будет присутствовать в системе, если инъекция пройдет через страницу веб-сайта, полученную из формы входа в систему. Шаг 4. Однако на следующем этапе в используемом браузере выполняется проверка расширения запроса с использованием элементов SQL. Шаг 5. После проверки этих элементов приложение автоматизации повторно вызовет его с помощью библиотечных запросов в библиотеке Python (php…). Это связано с тем, что функция отправки запроса СУБД MySQL (SQL) является типом Post, поскольку принцип работы системы основан на отправке через запрос, который был разработан. Шаг 6. После этого, если в функции возникнет ошибка, MBsi позволит получить доступ к веб-сайту через страницу входа. Шаг 7. Запрос, созданный приложением, позволяет найти в базе данных имя пользователя и пароль. Шаг 8. Инъекция выполняется с помощью функции подстроки, которая состоит из трех параметров, а именно имени, первого индекса и ряда символов. Шаг 9. Запрос на инъекцию соответствует основному запросу пространства в форме входа в систему, гарантируя, что основной запрос не будет работать. На этом этапе система не может заменить фактический запрос на инъекцию. Шаг 10. Выполняемые запросы автоматизируются по алгоритмам, приведенным в таблице выше. Первое, что нужно искать, это имя базы данных. Затем с этого имени начинается поиск списка таблиц. Шаг 11. После получения названия таблицы, пользователю разрешается доступ к таблицам, содержащим список имен пользователей и паролей.

Для выявления разделенных сетевых атак на эти базы после определения разделения распределенной базы данных пользователей корпоративной сети в разрезе территорий (полей) требуется вычислить матрицы парного сравнения на основе моделей, представленных в главе 3, в случае соответствия каждому из следующих уровней. Эти уровни:

- уровень активов в распределенной базе данных (a)
- уровень ресурсов в распределенной базе данных (R)
- уровень персонала в распределенной базе данных (H)
- уровень третьего лица в распределенной базе данных (U)
- уровень атаки в распределенной базе данных (Атака)
- уровень угроз в распределенной базе данных (T)
- уровень уязвимостей в распределенной базе данных (Z)
- уровень риска в распределенной базе данных (Риск).

Затем добавляются уровни обнаружения сетевых атак отдельных пользователей корпоративной сети на распределенную базу данных, а также дополнительные связи на уровне ресурсов и групп пользователей, а также между отделами.

$$A = \begin{pmatrix} 1 & a_1/a_2 & \dots & a_1/a_n \\ a_2/a_1 & 1 & \dots & a_2/a_n \\ \vdots & \vdots & \dots & \vdots \\ a_n/a_1 & a_n/a_2 & \dots & 1 \end{pmatrix}, \quad (1)$$

где A-матрица двойного сравнения уровней активов при обнаружении сетевых атак пользователей корпоративной сети на распределенную базу данных.

$$R = \begin{pmatrix} 1 & r_1/r_2 & \dots & r_1/r_k \\ r_2/r_1 & 1 & \dots & r_2/r_k \\ \vdots & \vdots & \dots & \vdots \\ r_k/r_1 & r_k/r_2 & \dots & 1 \end{pmatrix}, \quad (2)$$

где R-матрица двойного сравнения уровней ресурсов при обнаружении сетевых атак пользователей корпоративной сети на распределенную базу данных. Для остальных степеней вычисления выполняются в том же порядке, и результат определяется с помощью следующего выражения.

$$\text{Результат} = \begin{pmatrix} \sum_{j=1}^{n} a_j^c * \; r_i^c * h_i^c * \; u_i^c * huj_i^c * \; t_i^c * z_i^c * \; risk_1^c \\ \sum_{j=1}^{n} a_j^c * \; r_i^c * h_i^c * \; u_i^c * huj_i^c * \; t_i^c * z_i^c * \; risk_2^c \\ \sum_{j=1}^{n} a_j^c * \; r_i^c * h_i^c * \; u_i^c * huj_i^c * \; t_i^c * z_i^c * \; risk_s^c \end{pmatrix} \quad (3)$$

Выявление и устранение сетевых атак на распределенную базу данных пользователей корпоративной сети способствует повышению эффективности системы обеспечения информационной безопасности предприятия.

Атаки SQL-инъекций составили наибольшую часть атак на базу данных. Поэтому было бы целесообразно, если бы разработанный метод был протестирован в процессе обнаружения и устранения именно этого типа атак.

Разработанный методический алгоритм обнаружения такого рода атак реализован в следующей последовательности. При этом программа, разрабатываемая для обнаружения атаки, может быть реализована на любом языке программирования. Технология работы аналогична алгоритму IPS, главное отличие от которого заключается в том, что для команд вводится понятие веса, а решающий уровень решается именно на основе понятия веса. Чем важнее команда, тем больше в ней вес и соответственно требуется OTP (одноразовый пароль). Схема работы алгоритма представлена ниже. Шаг 1. Начало. Шаг 2. Получение идентификатора пользователя и пароля (OTP). Шаг 3. Анализ запроса (при этом уточняется, какая команда была дана через запрос, и получается т.е. Select/Insert/delete/Update). Шаг 4. Проверка веса запроса (при этом вес увеличивается в соответствии с частотой отправленного запроса, частота т.е. как быстро вес падает, если количество отправленных запросов уменьшается). Шаг 5. Выполняется условие проверки (т.е. условие следующее: Если вес равен или больше 3, переходите к шагу 6, в противном случае выполняйте условие перехода к шагу 9). Шаг 6. Проверяется командая (новая команда или нет). Шаг 7. Проверка по следующему условию (если запрос новый к шагу 8 в противном случае переход осуществляется к шагу 11, чтобы выполнить условие). Шаг 8. Если OTP подходит к шагу 9 в противном случае выполняется условйе перехода к шагу 11. Шаг 9. Выполнение запроса. Шаг 10. Сохранение учетной записи. Шаг 11. Конец.

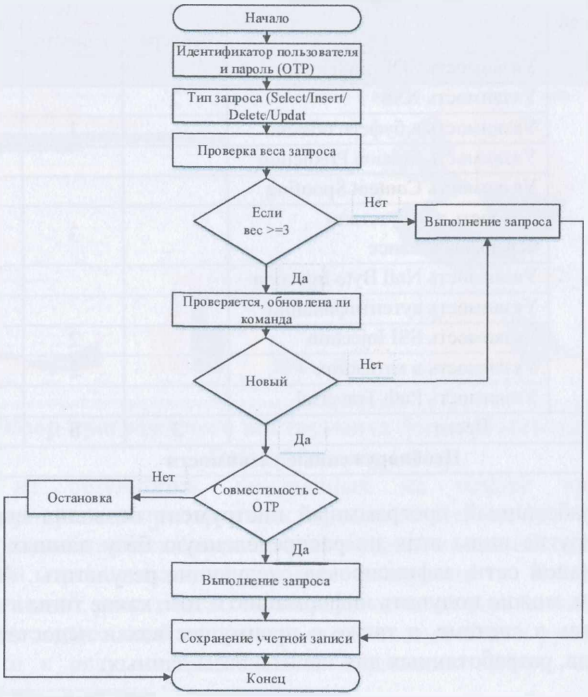


Рисунок 6. Блок-схема алгоритма обнаружения атаки SQL-инъекции.

Пятая глава диссертации, под названием **«Оценка эффективности системы обеспечения безопасности распределенных баз данных и результаты ее внедрения в практику»**, посвящена оценке эффективности метода обнаружения уязвимостей в распределенных базах данных, а также оценке эффективности метода обнаружения сетевых атак на распределенные базы данных пользователей корпоративных сетей и экспериментально-вычислительным результатам от внедрения разработанного программного средства в практику.

В ходе тестирования учитывались распределенные базы данных предприятия, СУБД, сервер, клиент и другие типы уязвимостей в среде, используемая пользователями предприятия для подключения к базе данных.

В связи с тем, что среда, в которой существуют уязвимости, разнообразна, возможность её дифференциации по типам при обнаружении уязвимостей включена в качестве модуля в дополнение к разработанному программному инструменту.

Таблица 2.

Результаты тестирования метода обнаружения уязвимостей в распределенной базе данных.

Общее количество уязвимостей	**Типы уязвимостей**	**Обнаруженная среда уязвимости**			**Всего**
		В сервере	В клиенте	В базе	
77	Уязвимость SQL-инъекции			57	57
	Уязвимость XSS	2			2
	Уязвимость в буфере обмена		1		1
	Уязвимость Session Prediction			1	1
	Уязвимость Content Spoofing			2	2
	Слабость в отсутствии перерыва в сеансе		3		3
	Уязвимость Null Byte Injection			3	3
	Уязвимость аутентификации	1			1
	Уязвимость SSI Injection		2		2
	Уязвимость в каталогах		2		2
	Уязвимость Path Traversal			1	1
Всего		**3**	**8**	**64**	**75**
Необнаруженные уязвимости					**2**

Разработанный программный инструмент позволил выявить сетевые атаки и другие виды атак на распределенную базу данных пользователей корпоративной сети, зафиксировав следующие результаты. Анализируя эти результаты, можно получить информацию о том, какие типы атак с привязкой увеличились в системе, а также о преимуществах и недостатках защитных механизмов, разработанных для защиты базы данных.

Таблица 3

Результаты тестирования метода обнаружения сетевых атак на распределенную базу данных пользователей корпоративной сети.

Название программного инструмента	Общее количество атак	Количество обнаруженных атак	Количество необнаруженных атак
Программный инструмент для обнаружения потенциальных атак на базу данных предприятия	9108	8935	173

Программное обеспечение системы безопасности распределенных баз данных обеспечивает безопасность базы данных, а также предоставляет следующие дополнительные возможности для системных администраторов. Исходя из этого, общий вид интерфейса программы, в котором объединены программные средства, разработанные на основе методов и алгоритмов ограничения разрешений, обнаружения уязвимостей в распределенной базе данных и обнаружения сетевых атак пользователей корпоративной сети на распределенную базу данных, представлен на рисунке 7.

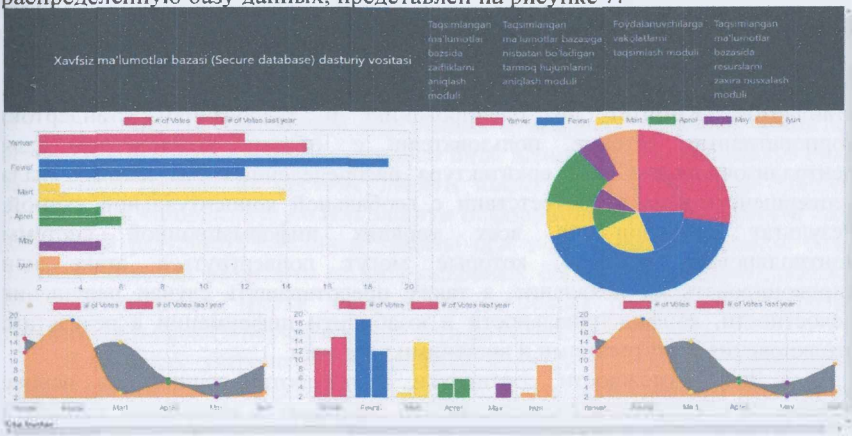


Рисунок 7. Обзор программного инструмента Secure Database (Secure Database).

Исходя из результатов, полученных на основе применения программного продукта на предприятиях отрасли, можно сказать, что в связи с тем, что распределенная база данных является одним из важнейших объектов добровольческой организации на момент внедрения и использования цифровых технологий, растет число возможных сетевых атак на нее.

Отсутствие надлежащей защиты от этих сетевых атак в нужное время может привести к ряду материальных и моральных потерь, а также к дискредитации предприятия.

ЗАКЛЮЧЕНИЕ

По результатам исследования диссертационной работы на тему «Методы и алгоритмы обеспечения безопасности распределенных баз данных пользователей корпоративных сетей» были представлены следующие выводы:

1. В целях обеспечения безопасности распределенной базы данных пользователей корпоративной сети был проведен сравнительный анализ типов сетевых атак на базу данных в корпоративной сети организации. На основе сравнительного анализа были выделены 4 основные классификации сетевых атак на базу данных с учетом внутренних и внешних угроз в отношении распределенной базы данных. Защита от этих сетевых атак предназначена для повышения эффективности системы, таких как степень их воздействия (высокий, средний, низкий), онлайн-и офлайн-реализация режима подключения (режим подключения зависит от типа внутренней и внешней сети), зависимость от типа СУБД, степень реализации (простая, сложная), нарушение конфиденциальности, нарушение целостности и нарушение удобства использования, а также предложен анализ на основе критериев. Анализ был предложен на основе таких критериев, как зависимость от типа МВВТ, уровня реализации (легкий, сложный), нарушения конфиденциальности, нарушения целостности и нарушения удобства использования.

2. Архитектура, разработанная для интеграции систем распределенных баз данных (ANSI / SPARC: американский Национальный институт стандартов, Комитет по планированию и требованиям стандартов) корпоративные сетевые пользователи с общим компонентом для централизованных СУБД архитектура распределенных баз данных была усовершенствована в соответствии с глобальной концептуальной схемой. Результат позволил на всех уровнях информационной системы контролировать объекты, которые могут подвергнуться атаке или спровоцировать их появление, а также предотвращать случаи нарушения целостности, конфиденциальности и юзабилити информации в результате столкновения с внутренними и внешними угрозами.

3. Для возможности сортировки и обработки данных на основе надежного обеспечения согласованности состояния и изменений данных, а также координации коллективной работы пользователей с общими данными в клиент-серверной архитектуре распределенной базы данных сформирована схема расположения компонентов информационной безопасности. В результате схема расположения компонентов информационной безопасности позволила своевременно обмениваться данными в четырех моделях технологий “клиент-сервер” и распределять информацию по таблицам в соответствии с привилегиями пользователей в общей базе данных организации с учетом вариаций компонентов.

4. Разработан метод и алгоритм резервного копирования ресурсов в распределенной базе данных с использованием возможности полного, инкрементального и дифференциального резервирования данных в базе

данных. Результат позволил разработать процесс резервного копирования с возможностью восстановления для распределенной базы данных и обеспечить согласованность, отказоустойчивость и эффективное восстановление данных, а также их адаптацию к различным условиям эксплуатации в режиме реального времени.

5. В целях управления процессом обеспечения безопасности распределенной базы данных пользователями корпоративной сети разработаны модели взаимодействия их информации в распределенной базе данных в процессе управления защищенными активами и управления ресурсами системы защиты информации на основе динамических экспертных систем поддержки принятия решений. Результат позволил осуществлять контроль над распределенной базой данных через единую систему защиты активов и ресурсов организации.

6. Исходя из механизмов управления использованием данных в распределенной базе данных, используемых в организации, усовершенствован модели управления рисками несанкционированного доступа и информационной безопасности в распределенной базе данных на основе аспектов управления использованием полномочий пользователей. Результат позволил пользователям при доступе к распределенной базе данных выявлять несанкционированные действия, выходящие за рамки полномочий, предоставленных организацией, и выявлять внутренние и внешние угрозы, осуществляемые на основе этих действий, а также управлять рисками в информационной системе.

7. Исходя из требований внутренних и внешних правовых актов по безопасности и защите распределенной базы данных, на основе заключения экспертной группы по системе защиты информации и объектам защиты разработана комплексная модель защиты информации в распределенной базе данных. В результате механизм защиты при защите распределенной базы данных позволил разделить ее на 4 основных блока информации (активы, ресурсы, персонал, третьи лица) и на их основе распределить угрозы, уязвимости и риски в корпоративной сети на логические группы.

8. В целях устранения имеющихся недостатков метода управления разрешениями RBAC в результате доработки с использованием атрибутов, используемых в методе управления разрешениями ABAC, были разработаны метод и алгоритм ограничения разрешений в распределенной базе данных. Результатом стало упрощение доступа пользователей к системе при ограничении разрешений, обеспечение масштабности и гибкости между распределенными узлами, предотвращение внутренних и внешних угроз, исходящих от пользователей, а также обеспечение конфиденциальности данных.

9. Разработан метод и алгоритм выявления уязвимостей в распределенной базе данных, основанный на использовании алгоритмов линейного, бинарного и интерполяционного поиска при выборе подходящих ответов на запросы, направляемые пользователями в базу данных. В

результате, несмотря на то, что таблицы в распределенной базе данных из-за распределения расположены в разных местах, можно выявить существующие уязвимости в среде информационной системы, то есть в серверной части, клиентской части или в части базы данных.

10. На основе введения понятия вес активов, ресурсов, персонала, третьей стороны, атак, угроз, уязвимостей и уровней риска в распределенной базе данных пользователей корпоративной сети усовершенствован метод и алгоритм обнаружения распределенных сетевых атак пользователей корпоративной сети на распределенную базу данных. Результат позволил выявить атаки, осуществляемые в отношении распределенной базы данных, и дифференцировать ошибки первого и второго типа с сетевыми аномалиями. Создана возможность устранения внутренних и внешних угроз корпоративной сети предприятия и сетевых атак, которые могут осуществляться на основе имеющихся уязвимостей в системе, в среде информационной системы.

11. Программный инструмент, разработанный на основе метода обнаружения уязвимостей в распределенной базе данных, позволил обнаруживать уязвимости в распределенной базе данных предприятия с точностью 97,5%. Это позволило выявить в общей сложности 77 уязвимостей в распределенной базе данных, разделив их на 5 основных типов, а также распределить их в среде информационной системы, то есть в разрезе серверной среды, клиентской среды и среды управления базами данных.

12. Программный инструмент, разработанный на основе метода обнаружения сетевых атак на распределенную базу данных пользователей корпоративной сети, позволил обнаружить 8935 из 9108 сетевых атак на распределенную базу данных предприятия с точностью 98,1 процента. Результат позволил обнаружить сетевые атаки на распределенную базу данных не только в среде информационной системы (сервер, клиент, база), но и на 8 уровнях распределенной базы данных предприятия (активы, ресурсы, персонал, третья сторона, атака, угроза уязвимости и уровни риска в распределенной базе данных).

13. Программное средство “Безопасная база данных (Secure Database)” (Государственный реестр программных продуктов Республики Узбекистан от 27.06.2023 г., Сертификата интеллектуальной собственности № 26031), разработанный на основе методов и алгоритмов ограничения разрешений, выявления уязвимостей в распределенной базе данных и обнаружения сетевых атак на распределенную базу данных пользователей корпоративной сети позволил обнаружить сетевые атаки с более высокой скоростью 1,8 микросекунд по сравнению с другими программными средствами, а также снизить количество случаев ложной активации системы в 1,6 раза.

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

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

SADIKOV SHUKHRAT MUKHAMADJANOVICH

METHODS AND ALGORITHMS FOR ENSURING THE SECURITY OF A DISTRIBUTED DATABASE OF CORPORATE NETWORK USERS

05.01.05 -Methods and systems of information protection. Information security

ABSTRACT OF THE DOCTORAL (DSc) DISSERTATION OF TECHNICAL SCIENCES

Tashkent -2023

The topic of the doctoral dissertation in technical sciences (DSc) is registered with the Higher Attestation Commission under the Ministry of Higher education, science and innovation of the Republic of Uzbekistan under No. B2023.3.DSc/T655.

The dissertation has been prepared at Tashkent University of Information Technologies.

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:	**Makhkamov Bakhtiyor Shukhratovich** doctor of economic sciences, professor
Official opponents:	**Kerimov Kamil Fikratovich** doctor of technical sciences, docent
	Jurayev Gayrat Umarovich doctor of physical and mathematical sciences, professor
	Primova Kholida Anarboyevna doctor of technical sciences, docent
Leading organization:	**Tashkent state technical university named after Islam Karimov**

The defense will take place «31» 10 2023 at 11.00 at 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. Ph.: (+99871) 238-64-43, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of Tashkent University of Information Technologies (is registered under № 238) (Address: 100084, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43.

Abstract of dissertation sent out on «20» 10 2023 y.
(Dispatching protocol № 4 on «19» 10 2023 y).

D.Y. Irgasheva
Deputy Chairman of the scientific council awarding scientific degrees, doctor of technical sciences, professor

E.Sh. Nazirova
Scientific secretary of scientific council awarding scientific degrees, doctor of technical sciences, professor

S.K. Ganiyev
Chairman of the scientific seminar at the scientific council for the awarding of academic degrees, doctor of technical sciences, professor

INTRODUCTION (abstract of doctoral dissertation (DSc))

The aim of the research work is to develop effective methods and algorithms for detecting vulnerabilities and network attacks in a distributed database of corporate network users, allowing to increase the efficiency of the distributed database protection system.

The object of the research work is the process of protecting a distributed database of users of corporate networks of the Republic of Uzbekistan.

The scientific novelty of the research work is as follows:

improved architecture designed to integrate distributed database systems (ANSI/SPARC: American National Standards Institute, Standards Planning And Requirements Committee) corporate network users with a common component for centralized DBMS distributed database architecture in accordance with the global conceptual framework;

a method and algorithm for backing up resources in a distributed database has been developed using the possibility of full, incremental and differential backup of data in the database;

models for the interaction of its information in a distributed database based on dynamic expert decision support systems for managing protected assets and resource management of the information security system have been developed;

models for managing risks of unauthorized access and information security in a distributed database have been improved based on mechanisms for managing the use of data in a distributed database used in the organization, based on aspects of managing the use of user powers;

a comprehensive model for protecting information in a distributed database has been developed based on the requirements of internal and external legal acts on the security and protection of information in a distributed database, based on the conclusion of an expert group on the internal and external parameters of shared resources for the information security system and protected objects;

a method and algorithm for detecting vulnerabilities in a distributed database has been developed, based on the use of linear, binary and interpolation search algorithms when selecting in tables the appropriate answers to queries sent by users to the database;

the method and algorithm for detecting separated network attacks on a distributed database of corporate network users has been improved based on the introduction of the concept of the weight of assets on resources, personnel, third parties, attacks, threats, vulnerabilities and risk levels in a distributed database of corporate network users.

Implementation of research results. Based on scientific results obtained on methods and software for ensuring the security of distributed databases of corporate network users:

a developed software tool for integrating distributed database systems (ANSI/SPARC: American National Standards Institute, Standards Planning and Requirements Committee) on the architecture of distributed databases of users of corporate networks with a common component for centralized DBMS, introduced into

the practical activities of the State Unitary Enterprise "Cyber Security Center" (reference of the Ministry of Digital Technologies No. 33-8/5665 dated August 18, 2023). A scientific study showed that a software tool developed based on a method for detecting vulnerabilities in a distributed database allowed identifying 77 vulnerabilities of 5 main types in a distributed enterprise database with an accuracy of 97.5%;

a software tool developed on the basis of a method and algorithm for backing up resources in a distributed database in real time using the possibility of full, incremental and differential backup of data in the database, introduced into the practical activities of the State Unitary Enterprise "Cyber Security Center" (reference of the Ministry of Digital Technologies No. 33-8/5665 dated August 18, 2023). The scientific study identified 8,935 of 9,108 possible network attacks on an enterprise's distributed database with an accuracy of 98.1 percent.

a software tool developed on the basis of models of information interaction in a distributed database in the process of resource management of the information management and protection system, protected by level of use, based on dynamic expert decision support systems, introduced into the practical activities of the limited liability company "UZINFOCOM" (reference of the Ministry of Digital Technologies No. 33-8/5665 dated August 18, 2023). The scientific study made it possible to identify 76 vulnerabilities of 6 main types in a distributed enterprise database with an accuracy of 98.2%, and also to identify 7560 out of 7683 network attacks on a distributed enterprise database with an accuracy of 98.3%;

a software tool developed on the basis of models for managing the risks of unauthorized access and information security in a distributed database based on aspects of managing the use of user powers, based on the mechanisms used in the organization to manage the use of information in a distributed database, has been introduced into the practical activities of the limited liability company "UZINFOCOM" (reference of the Ministry of Digital Technologies No. 33-8/5665 dated August 18, 2023). A comparison with the applied software tools in order to determine the effectiveness of this software tool showed that, compared with other software tools, the speed of detecting network attacks is 2.1 microseconds higher, and the number of cases of false system startup is 1.7 times less;

a software tool developed on the basis of a comprehensive model of information protection in a distributed database based on the conclusion of an expert group on the information protection system and protection objects on the internal and external parameters of shared resources, based on the requirements of internal and external legal acts on security and information protection, has been put into practice activities of the State Unitary Enterprise "CEMC" (reference of the Ministry of Digital Technologies No. 33-8/5665 dated August 18, 2023). The scientific study made it possible to identify 84 vulnerabilities of 6 main types in a distributed enterprise database with an accuracy of 97.1%, and also to identify 6417 out of 6574 network attacks on a distributed enterprise database with an accuracy of 97.6%;

Structure and volume of the dissertation. The dissertation consists of an introduction, five chapters, a conclusion, a list of references and appendices. Dissertation volume – 191 pages.

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

I bo'lim (I chast; part I)

1. Sadikov Sh.M., Comparative analysis of database security assurance models from unauthorized actions and quantitative assessment of integrity, Texas Journal of Engineering and Technology, 2023, pp. 14-18 (OAK (23) Scientific Journal Impact Factor 6,788).

2. Sadikov Sh.M., The concept of providing information security in distributed system of organizational database, "Science and Education in Karakalpakstan" 2023 №2/2. pp. 69-74. (05.00.00; №27)

3. Sadikov Sh.M., Analysis of Existing Vulnerabilities in Information Reception, Processing and Transmission Systems in a Distributed Database, Eurasian Journal of Engineering and Technology, 2023, pp. 1-4 (OAK (23) Scientific Journal Impact Factor 7,985).

4. Sadikov Sh.M., Options for organizing data hierarchy in relational systems, "Muhammad al-Xorazmiy avlodlari" Ilmiy amaliy va axborot – tahliliy jurnali 4(22)/2022. pp. 163-164 (05.00.00; №10).

5. Sadikov Sh.M., Optimal data placement and optimality criteria, "Muhammad al-Xorazmiy avlodlari" Ilmiy amaliy va axborot – tahliliy jurnali 2(20)/2022. pp. 226-228 (05.00.00; №10).

6. Sadikov Sh.M., Korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash usullari. Monografiya. 2023. 128 b.

7. Sadikov Sh.M. Interaction management model data in the information security system, "Muhammad al- Xorazmiy avlodlari" ilmiy amaliy va axborot tahliliy jurnali, 2(24)/2023. -B. 158-164 (05.00.00; №10).

8. Sadikov Sh.M., Development of algorithms and consctruction methodssecure personal data information systems, "Muhammad al-Xorazmiy avlodlari" Ilmiy amaliy va axborot – tahliliy jurnali 1(23)/2023. pp. 219-223 (05.00.00; №10).

9. Sadikov Sh.M. Information security risk and threat management process data model, "Muhammad al- Xorazmiy avlodlari" ilmiy amaliy va axborot tahliliy jurnali, 2(24)/2023. -B. 3-8 (05.00.00; №10).

10. Sadikov Sh.M., Organitation of mechanism for limiting the use of the organization's database role-based access control model, "Science and Education in Karakalpakstan" 2023 №2/2. pp. 41-45 (05.00.00; №27).

11. Sadikov Sh.M., Permission pertriction method and algorithm in distributed database, Spectrum Journal of innovation, reforms and development, 2023. –P. 29-36 (OAK (23) Scientific Journal Impact Factor 7,255).

12. Sadikov Sh.M., Method of algorithm for determining weaknesses in a distributed database, A peer Reviewed, Open access, International journal, 2023. P. 22-29 (OAK (23) Scientific Journal Impact Factor 7,852).

13. Sadikov Sh.M., Method and algorithm for detecting network attacks on

the distributed database of corporate network users, European Journal of Interdisciplinary Research and Development, Volume-18. 2023. –P. 111-120 (OAK (23) Scientific Journal Impact Factor 7,985).

II bo'lim (I chast; part I)

14. Sadikov Sh.M., Korporativ tarmoqdagi taqsimlangan ma'lumotlar bazasi xavfsizligini ta'minlash, International Scientific and Technical Conference "Digital Technologies: Problems and Solutions for Practical Implementation in an Industry" on April 27-28, 2022. B. 246-247.

15. Sadikov Sh.M., Ma'lumotlar bazasida ma'lumotlarni tashkil etishning modellari, International Scientific and Technical Conference "Digital Technologies: Problems and Solutions for Practical Implementation in an Industry" on April 27-28, 2022. B. 241-243.

16. Sadikov Sh.M., Korporativ tarmoqda ma'lumotlar bazasiga bo'ladigan tarmoq hujum turlari, International Scientific and Technical Conference "Digital Technologies: Problems and Solutions for Practical Implementation in an Industry" on April 27-28, 2022. B. 244-246.

17. Sh.M. Sadikov, Description and classification of information security threats in the database, International conference: Recent advance in intelligent information and communication technologies, Tashkent 2022. pp. 290-293.

18. Sadikov Sh.M., Taqsimlangan ma'lumotlar bazasi arxitekturasi, Ilm-fan va innovatsiya ilmiy –amaliy konfrensiya, 2023. pp. 144-146.

19. Sadikov Sh.M., Client-server architecture of distributed database, Ilm-fan va innovatsiya ilmiy –amaliy konfrensiya, 2023. pp. 140-143.

20. Sadikov Sh.M., Taqsimlangan ma'lumotlar bazasining mijoz-server arxitekturasida axborot xavfsizligi komponentalarining joylashuv sxemasi ishlab chiqish, Ilm-fan va innovatsiya ilmiy –amaliy konfrensiya, 2023. pp. 81-84.

21. Sadikov Sh.M., Distributed database backup technologies, Innovative research in modern education, Hosted fram Toronto, Canada 2023, pp. 45-47.

22. Sh.M. Sadikov, Vulnerability analysis of information processing technologies in the database, International conference: Recent advance in intelligent information and communication technologies, Tashkent 2022. pp. 327-332.

23. Sadikov Sh.M., Development of modular architecture of distributed database of corporate network, Academic international conference: Multi-Disciplinary studies and education, Pittsburgh, USA 2023, pp. 1-4.

24. Sadikov Sh.M., Classification of information security threats in the database, International conference: Innovative research in modern education, Toronto, Canada 2023, pp. 50-51.

25. Sadikov Sh.M., Protection of databases in corporate information systems, Academic international conference: Multi-Disciplinary studies and education, Pittsburgh, USA 2023, pp. 120-121

26. Sh.M.Sadikov, B.Sh.Maxkamov "Xavfsiz ma'lumotlar bazasi (Secure database) dasturiy vositasi" // Dasturga guvohnoma № DGU 26031, Toshkent,

27.06.2023 y.

27. Sh.M.Sadikov, B.Sh.Maxkamov "Korxonaning ma'lumotlar bazasiga bo'ladigan hujumlarni bartaraf etish dasturiy vositasi" // Dasturga guvohnoma № DGU 26032, Toshkent, 27.06.2023 y.

28. Sh.M.Sadikov, B.Sh.Maxkamov "Korxonaning ma'lumotlar bazasiga bo'ladigan hujumlarni aniqlash dasturiy vositasi" // Dasturga guvohnoma № DGU 26033, Toshkent, 27.06.2023 y.

Avtoreferat «Muhammad al-Xorazmiy avlodlari» Ilmiy-amaliy va axborot tahliliy jurnali tahririyatida tahrirdan o'tkazildi hamda o'zbek, rus va ingliz tillaridagi matnlar o'zaro muvofiqlashtirildi.

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog'i: 3,75. Adadi 100 dona. Buyurtma № 52/23.

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