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

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

IBROHIMOV AZIZBEK RAVSHANBEK O‘G‘LI

VEB – SERVERLARDAGI AXBOROTNI TARMOQ HUJUMLARIDAN HIMOYALASH USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent-2024

UDK: 004.056.57

Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам

Contents of dissertation abstract of the doctor of philosophy (PhD) on technical sciences

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

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

IBROHIMOV AZIZBEK RAVSHANBEK O‘G‘LI

VEB – SERVERLARDAGI AXBOROTNI TARMOQ HUJUMLARIDAN HIMOYALASH USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent-2024

Texnika fanlari bo'yicha falsafa doktori (PhD) dissertatsiyasi mavzusi O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2023.3.PhD/T4056 raqam bilan ro'yxatga olingan.

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

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

Ilmiy rahbar:	**Xamdamov Rustam Xamdamovich** texnika fanlari doktori, professor
Rasmiy opponentlar:	**Jurayev Gayrat Umarovich** fizika-matematika fanlari doktori, dotsent
	Nasrullayev Nurbek Baxtiyorovich texnika fanlari bo'yicha falsafa doktori, dotsent
Yetakchi tashkilot:	**"UNICON.UZ" - Fan – texnika va marketing tadqiqotlar markazi MChJ**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.02 raqamli Ilmiy kengashning 2024-yil "14" yanvar soat 11⁰⁰ dagi majlisida bo'lib o'tadi. (Manzil: 100084, Toshkent shahri, Amir Temur ko'chasi, 108-uy. Tel.: (99871) 238-64-43, e-mail: tuit@tuit.uz).

Dissertatsiya bilan Toshkent axborot texnologiyalari universiteti Axborot-resurs markazida tanishish mumkin (295 raqam bilan ro'yxatga olingan.). (Manzil: 100084, Toshkent shahri, Amir Temur ko'chasi, 108-uy. Tel.: (99871) 238-64-43).

Dissertatsiya avtoreferati 2024-yil "12" yanvar da tarqatildi.
(2024-yil "11" yanvar dagi 4 raqamli reestr bayonnomasi.)

B.Sh. Maxkamov
Ilmiy darajalar beruvchi ilmiy kengash raisi, i.f.d., professor

M.S. Saitkamolov
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, i.f.d., dotsent

S.K. Ganiyev
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi ilmiy seminar raisi, t.f.d., professor

KIRISH (falsafa doktori (PhD) dissertatsiyasining annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahonda korxona va tashkilotlar uchun xalqaro bozor munosabatlarini amalga oshirishda ular joylashgan hududda internetga ulanish imkoni mavjud bo‘lsa shuni o‘zi yetarli hisoblanadi. Korxona va tashkilotlarning xalqaro va milliy sahnalardagi yuzi bu ularning rasmiy veb sahifalaridir. Shuning uchun ham veb server va veb ilovalarga qaratilgan hujumlar soni kundan kunga ortib bormoqda. “Kaspersky kompaniyasi ma’lumotlariga ko‘ra, veb serverga bo‘lgan hujumlar soni keskin ortgan bo‘lib, oxirgi bir yil ichida 687 861 449 ta hujumlar aniqlangan va ularning asosiy qismi 10 ta davlatga to‘g‘ri kelgan”[1] . Bu xorijiy mamlakatlar, Chexiya, AQSH, Germaniya, Gollandiya, Fransiya, Rossiya Federatsiyasi va boshqa davlatlardir. Ushbu mamlakatlarda hamda boshqa davlatlarda veb serverlardagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlarini ishlab chiqish hamda tashkilotning veb serverini himoyalash tizimlarini takomillashtirish muhim ahamiyat kasb etmoqda.

Jahonda veb-serverlardagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlarini takomillashtirishga hamda neyron tarmoqlar yordamida hujumlarni aniqlashga yo‘naltirilgan ilmiy-tadqiqot ishlari olib borilmoqda. Bu borada, jumladan veb interfeysga qaratilgan tarmoq hujumlarni aniqlash usullarini ishlab chiqish muhim vazifalardan biri hisoblanmoqda. Shu bilan birga, veb serverdagi barcha baglarni aniqlashni yagona yechimi bo‘lmaganligi sababli, veb serverdagi ochiq qolgan portlar va zaifliklarni aniqlash uchun zamonaviy usullardan foydalanib himoya mexanizmini ishlab chiqish zarur bo‘lmoqda.

Respublikamizda davlat va xo‘jalik boshqaruv organlarida veb serverga qaratilgan hujumlardan himoyalanish uchun keng qamrovli chora-tadbirlar amalga oshirilmoqda. 2022-2026-yillarga mo‘ljallangan Yangi O‘zbekistonning Taraqqiyot strategiyasi to‘g‘risida, jumladan “... “UZ” domen zonasi Internet-makonining kiberxavfsizligini ta’minlashning…” vazifalari belgilangan. Mazkur vazifalarni amalga oshirishda, veb-serverlardagi axborotni tarmoq hujumlaridan himoyalashning zamonaviy usullarni qo‘llash va veb serverni himoyalashda yangi tizimlardan foydalanish muhim vazifalardan biri hisoblanadi.

O‘zbekiston Respublikasi Prezidentining “2022-2026-yillarga mo‘ljallangan Yangi O‘zbekistonning Taraqqiyot strategiyasi to‘g‘risida”[2]gi, 2022-yil 28-yanvardagi PF-60-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

[1] https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_rus.pdf

[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

me’yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya tadqiqoti ma’lum darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishi-ning ustuvor yo‘nalishlariga mosligi. Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Veb server va ilovalar xavfsizligini ta’minlashda zaifliklarni aniqlash usuli va zamonaviy usullarni qo‘llagan holda veb serverdagi ochiq portlarni va zaifliklarni aniqlash uchun ishlab chiqilgan usullar va algoritmlarni axborot xavfsizligini ta’minlashda qo‘llash bo‘yicha A.Stasyuk, A.Korchenko, M.Satton, A.Grin, P.Amini, M.V.Sherba, D.Y.Gamayunov, I.S.Aleksandrov va boshqa chet ellik olimlar tomonidan ilmiy izlanishlar olib borilmoqda. Veb-serverlardagi axborotni tarmoq hujumlaridan himoyalashda guruhlash usulini qo‘llagan holda Skinner Kris, SH.Harris, A.Antonov, Brian Krebs, Satalin Simpanu ilmiy izlanishlar olib borishgan. Bundan tashqari, Tadviser, OWASP, Kaspersky kabi tashkilotlari tomonidan zamonaviy usullarni qo‘llash orqali veb-serverlardagi axborotni tarmoq hujumlaridan himoyalashning dasturiy-apparat vositalarini ishlab chiqish bo‘yicha injenerlik-tadqiqot ishlari olib borilmoqda.

O‘zbekistonda akademik T.F.Bekmuratov tomonidan veb-serverlardagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlarini ishlab chiqish bo‘yicha ilmiy izlanishlar olib borilgan va hozirda S.K.Ganiyev, R.X.Xamdamov, M.M.Karimovlar boshchiligidagi ilmiy jamoalar tomonidan ilmiy izlanishlar olib borilmoqda.

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-1-2018-1-RO-EPPKA2-CBHE-JP “Developing Services for Individuals with Disabilities” mavzusidagi loyiha doirasida bajarilgan.

Tadqiqot maqsadi veb serverni himoyalash tizimining samaradorligini oshirishga imkon beruvchi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlarini ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

veb serverlardagi axborotni tarmoq hujumlaridan himoyalash usullarini qiyosiy tahlil qilish va zaifliklarni aniqlash tizimining strukturasini ishlab chiqish;

veb serverlardagi zaifliklarni aniqlashning uch bosqichli testlash usulini ishlab chiqish;

veb serverlardagi zaifliklarni guruhlash usuli va algoritmini ishlab chiqish;

veb interfeysga qaratilgan tarmoq hujumlarini aniqlash usuli va algoritmini ishlab chiqish.

Tadqiqotning obyekti sifatida veb serverdagi zaifliklarni aniqlash va axborotni tarmoq hujumlaridan himoyalash jarayoni olingan.

Tadqiqotning predmetini veb serverdagi zaifliklarni aniqlash va axborotni tarmoq hujumlaridan himoyalash usul va algoritmlari tashkil etadi.

Tadqiqot usullari. Tadqiqot jarayonida neyron tarmoqlar, ehtimollik nazariyasi, vektor formati, graflar nazariyasi, diskret matematika usullaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

xalqaro tashkilotlar tomonidan jamlangan va hozirda ma'lum bo'lgan axborot xavfsizligi zaifliklarining ma'lumotlar bazasi asosida veb serverdagi zaifliklarni yagona identifikator tizimi orqali zaifliklarni mavjud bo'lish muhitiga ko'ra guruhlaydigan veb serverlardagi zaifliklar reyestri shakllantirilgan;

veb serverlardagi ilovalarni ekvivalentlik, chegara va qarorlar jadvali testlarining kombinatsiyalashgan varianti asosida real vaqt rejimida testlashga ko'ra ilovalardagi zaifliklarni aniqlashning uch bosqichli testlash usuli ishlab chiqilgan;

veb serverda mavjud bo'lgan aloqa kanali, protokoli va apparat platforma muhitiga ko'ra veb serverning umumlashgan paramertlar guruhini yaratish asosida har bir parametr darajasiga mos keladigan veb serverlardagi zaifliklarni guruhlash usuli va algoritmi ishlab chiqilgan;

veb serverga yuborilgan so'rovlarning statistik tuzilmasi va veb sahifalarni mantiqiy toifalarini hisobga olgan holda shakllantirilgan so'rov vektor formati asosida veb interfeysga qaratilgan tarmoq hujumlarini aniqlash usuli va algoritmi ishlab chiqilgan;

veb serverga bo'ladigan tarmoq hujumlarini veb serverning umumlashgan paramertlar guruhlari asosida xavfsiz holatga keltirish natijasida zaifliklarning mavjud bo'lish sathida ishlaydigan protokoliga ko'ra tarmoq hujumlarini aniqlashning VITE usuli va algoritmi ishlab chiqilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

veb serverdagi zaifliklarni aniqlash asosida axborotni tarmoq hujumlaridan himoyalashning dasturiy vositasi ishlab chiqilgan;

veb-ilovalardagi zaifliklarni topish va veb-ilovalarni hujum vektorlaridan himoya qilish uchun TCP/IP protokoli darajasida ishlaydigan veb-ilovalarning zamonaviy himoyasini tashkil etish asosida tarmoqlararo ekran takomillashtirilgan.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalarining ishonchliligi tashkilot veb serverlardagi zaifliklarni aniqlash, guruhlash, veb interfeysga qaratilgan tarmoq hujumlarini aniqlash, tarmoq hujumlarini aniqlash usullaridan turli sharoitlarda olingan real hamda tajribaviy tahlil natijalari bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati ishlab chiqilgan veb serverlardagi zaifliklarni aniqlash bosqichlari usuli va algoritmi, veb serverlardagi zaifliklarni aniqlashning uch bosqichli testlash usuli va algoritmini ishlab chiqish, veb interfeysga qaratilgan tarmoq hujumlarini aniqlash usuli va algoritmi hamda tarmoq hujumlarini aniqlashning VITE usuli va algoritmi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati taklif etilgan usullar va algoritmlar asosida ishlab chiqilgan dasturiy vositaning tashkilot veb serveridagi zaifliklarni aniqlash va axborotni tarmoq hujumlaridan himoyalash jarayonini samaradorligini ortishiga ko'maklashishi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Veb-serverdagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlari hamda dasturiy vositalari bo‘yicha olingan ilmiy natijalar asosida:

veb-serverdagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlari asosida ishlab chiqilgan dasturiy vosita “Kiberxavfsizlik markazi” davlat unitar korxonasining amaliy faoliyatiga joriy qilingan (Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining 2022-yil 11-oktabrdagi 33-8/6723-son ma’lumotnomasi). Ilmiy tadqiqot natijasi korporativ tarmoqdagi 152348 ta tarmoq hujumlarnini 98.7% aniqlik va 1.3% xatolik qayd etgan holda aniqlash imkonini bergan;

veb-serverdagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlari asosida ishlab chiqilgan dasturiy vosita “UZINFOCOM Davlat axborot tizimlarini yaratish va qo‘llab-quvvatlash bo‘yicha yagona integrator” mas’uliyati cheklangan jamiyatining amaliy faoliyatiga joriy qilingan (Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining 2022-yil 11-oktabrdagi 33-8/6723-son ma’lumotnomasi). Ilmiy tadqiqot natijasida tashkilotning veb serveridagi 153 ta ochiq portni va 6 turdagi zaifliklarni hamda 163469 ta tarmoq hujumlarini 97.9% aniqlik va 2.1% xatolik qayd etgan holda aniqlash imkonini bergan;

veb-serverdagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlari asosida ishlab chiqilgan dasturiy vosita “MAXSUS XIZMAT BUX” mas’uliyati cheklangan jamiyatining amaliy faoliyatiga joriy qilingan (Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining 2022-yil 11-oktabrdagi 33-8/6723-son ma’lumotnomasi). Ilmiy tadqiqot natijasi tashkilot veb serveridagi 148 ta ochiq portni va 6 turdagi zaifliklarni hamda 135238 ta tarmoq hujumlarini 97.5% aniqlik va 2.5% xatolik qayd etgan holda aniqlash imkonini bergan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 2 ta xalqaro va 2 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Dissertatsiyaning mavzusi bo‘yicha jami 18 ta ilmiy ish chop etilgan, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarida 6 ta maqola, shulardan, 3 tasi xorijiy va 3 tasi respublika jurnallarida nashr etilgan hamda 3 ta EHM uchun yaratilgan dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, to‘rtta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiya hajmi 115 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi va zaruriyati asoslangan, tadqiqotning O‘zbekiston Respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, maqsad va vazifalari belgilab olingan hamda tadqiqot obyekti va predmeti aniqlangan, olingan natijalarning ishonchliligi asoslab

berilgan, ularning nazariy va amaliy ahamiyati, tadqiqot natijalarini amalda joriy qilish holati, nashr etilgan ishlar va dissertatsiyaning tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning **“Veb serverlardagi axborotga bo‘ladigan tarmoq hujum turlari va ulardan himoyalanish usullari tahlili”** deb nomlangan birinchi bobida veb serverlardagi axborotga bo‘ladigan tarmoq hujum turlari, ularninig bir-biridan farqi hamda veb serverlardagi zaifliklarni aniqlash usullari tahlili va veb serverlardagi axborotni tarmoq hujumlaridan himoyalash usullarining qiyosiy tahlili keltirilgan.

Birinchi paragrafda veb serverlardagi axborotga bo‘ladigan tarmoq hujum turlari va axborotga ta’sir qiluvchi xavfsizlik tahdidlari qaratilgan obyektlar hamda hujumga uchragan foydalanuvchilar ulushi bo‘yicha birinchi 10 ta mamlakat foydalanuvchilari bilan bir qatorda veb-hujum manbalarini mamlakatlar bo‘yicha taqsimlanishi tahlil qilingan.

Ikkinchi paragrafda veb serverlardagi zaifliklarni aniqlash usullarining afzalliklari va kamchiliklari hamda zaifliklarni aniqlashda foydalaniladigan testlash usullari kim tomonidan amalga oshirilishi, dasturlash bo‘yicha bilim talab etilishi, amalga oshirish bo‘yicha bilim talab etilishi hamda sinov holatlari uchun asosiy manbasiga ko‘ra qiyosiy tahlil qilindi. Qiyosiy tahlil natijalariga qo‘ra qora quti usulini samaradorligi yuqori ekanligi aniqlangan.

Uchinchi paragrafda veb serverlardagi axborotni tarmoq hujumlaridan himoyalash usullarini afzalliklari va kamchiliklarini aniqlash maqsadida ularni ikkita guruhga, host darajasidagi tarmoq hujumlari va tarmoq darajasida tarmoq hujumlarini aniqlash usullariga ajratib olingan. Tarmoq darajasidagi tarmoq hujumlarni amalga oshirishda OSI modelining 7 ta sathida ma’lumot ko‘rinish muhim ahamiyat kasb etganligi sababli ikkita guruh uchun alohida-alohida qiyosiy tahlil amalga oshirilgan. Qiyosiy tahlil natijasida tarmoq darajasida tarmoq hujumlarini aniqlash usullarining samadorligi yuqori ekanligi aniqlangan.

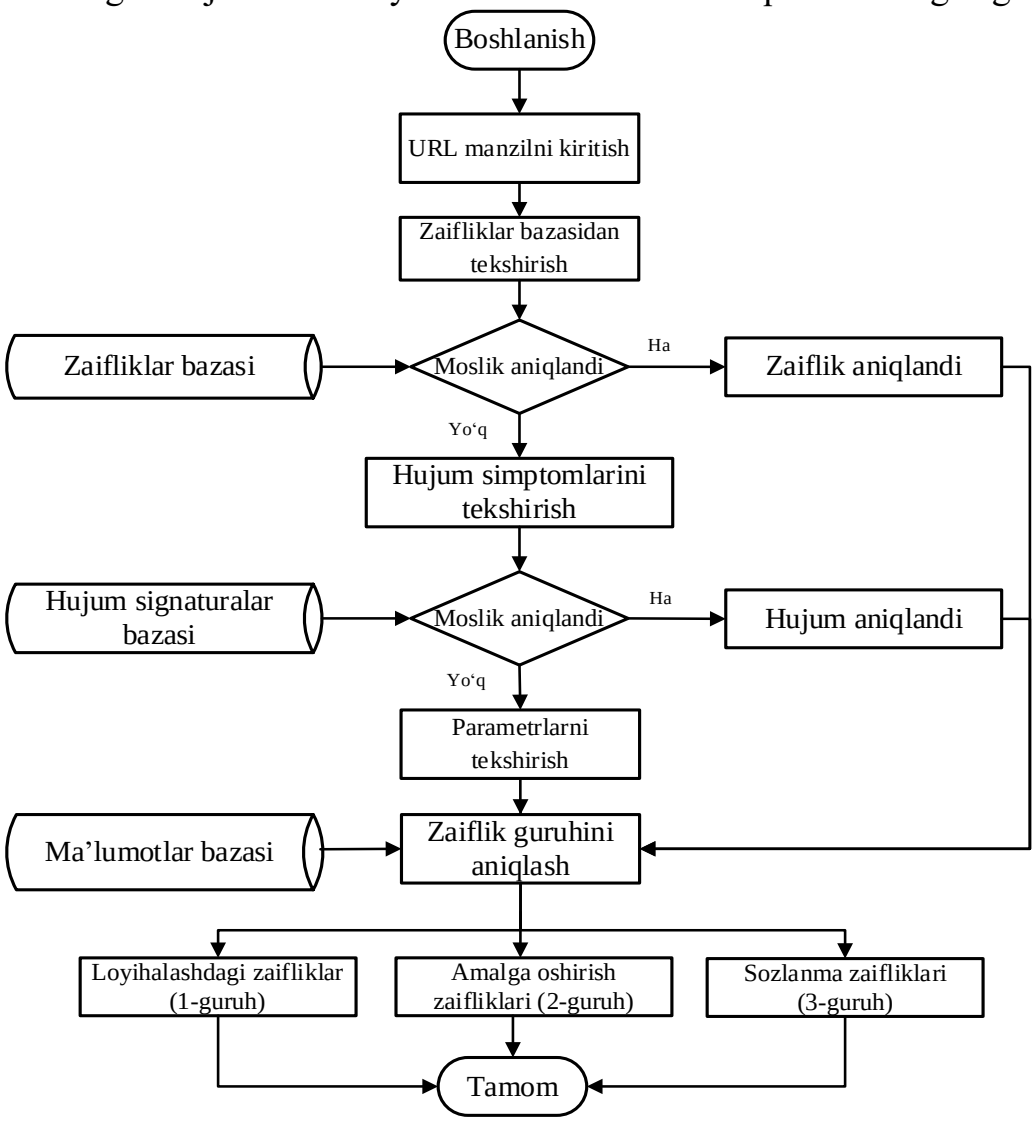
Dissertatsiyaning **“Veb serverlardagi zaifliklarni aniqlash va guruhlash usullari va algoritmlari”** deb nomlangan ikkinchi bobida veb serverlardagi zaifliklarni aniqlash tiziminig amalda foydalanib kelinayotgan va zamonaviy strukturalari, veb serverlardagi zaifliklarni aniqlash bosqichlari usuli va algoritmi hamda veb serverlardagi zaifliklarni guruhlash usuli va algoritmi ishlab chiqilgan.

Mazkur bobning *birinchi paragrafida* US-CERT, Open Information Security Foundation tashkiloti tomonidan shakllantirilgan statistik ma’lumotlar asosida dasturiy mahsulot ishlab chiquvchilarning dasturlaridagi zaifliklarini bitta identifikator tizimida (masalan, CVE-ID) guruhlaydigan veb serverlardagi zaifliklarni reyestri shakllantirildi hamda veb serverlardagi mavjud zaifliklarni aniqlash tizimining zamonaviy strukturasi ishlab chiqildi. Natijada veb serverlardagi zaifliklar va ular asosida amalga oshiriladigan hujum turlarini OWASP ning zaifliklar bazasiga integratsiya qilish imkonini bergan.

Ikkinchi paragrafda Uch sinfdan iborat veb ilovalarni testlash usuli ekvivalentlik testini 4 ta bosqichda, chegara testini 9 bosqichda va qarorlar jadvali testini 5 ta bosqichda amalga oshirish asosida veb serverlardagi zaifliklarni aniqlashning uch bosqichli testlash usuli va algoritmi ishlab chiqilgan. Natijada veb

server va ilovalardagi zaifliklarni aniqlash uchun har xil turdagi ma’lumotlar to‘plamiga to‘liq kirish imkonini bergan. Uch bosqichli testlash usuli zaifliklarni aniqlash bilan bir qatorda ularni bartaraf etish va axborotni himoya qilish hamda veb serverlardagi ilovalarga o‘z vaqtida texnik xizmat ko‘rsatishga imkon berdi.

Uchinchi paragrafda aloqa kanali, protokoli, www server ishlaydigan apparat platformasi va operatsion tizimi hamda veb server ma’lumotlar bazasini boshqarish tizimidagi va shu kabi zaifliklarni asosiy uchta katta guruhlarga ajratib olish hamda ushbu guruhlarga kiradigan zaifliklarni ma’lum ketma-ketliklar asosida umumlashgan guruhlarini yaratish imkonini beradigan veb serverlardagi zaifliklarni guruhlash usuli va algoritmi ishlab chiqildi. Natijada har bir zaiflik asosida amalga oshiriladigan hujum uchun himoya mexanizmi emas balki zaifliklarni guruhiga tegishli bo‘lgan hujumlar himoya mexanizmi ishlab chiqish imkoniga ega bo‘lindi.



1-rasm. Veb serverdagi zaifliklarni guruhlash algoritmining blok sxemasi

Veb serverni zaifliklari to‘plami uning barcha tarkibiy qismlarini zaifliklari to‘plamidan iborat, ya’ni

$$Z_s = \bigcup_{i=1}^{n} \bigcup_{j=1}^{3} Z_{ij}, \qquad (1)$$

Bu yerda Z_s – butun axborot tizimini zaifliklari to‘plami;

Z_{ij} – guruhlashtirishni j-sathi axborot tizimini i-obyektini zaifliklari to‘plami;

n – veb serverdagi mavjud obyektlarni umumiy soni;

$m(i,j)$ - guruhlashtirishni j- sathi axborot tizimini i-obyekt zaifliklariga amalga oshiriladigan ehtimoliy hujumlarning umumiy soni.

Veb serverni hujumga ehtimoliy reaksiyalari to‘plamini quyidagi ifodadan olish mumkin:

$$T_{ER} = \bigcup_{i=1}^{n} \bigcup_{j=1}^{3} \bigcup_{k=1}^{m(i,j)} \bigcup_{e=1}^{l(i,j,k)} T_{ijke}, \qquad (2)$$

Bu yerda T_{ER} – hujumga ehtimoliy reaksiyalar to‘plami;

T_{ijke} - guruhlashtirishni j-sathi axborot tizimin i-obyektini zaifligiga uyushtiriladigan k-hujumga reaksiyalar to‘plami;

n – veb serverdagi mavjud obyektlarini umumiy soni;

$m(i,j)$ - guruhlashtirishni j-sathi i-obyekti zaifliklariga amalga oshiriladigan ehtimoliy hujumlarning umumiy soni;

$l(i,j,k)$ - i,j va k parametrlari bilan xarakterlanadigan hujumga ehtimoliy reaksiyalarni umumiy soni.

Dissertatsiya ishining **“Veb – serverlarga bo‘ladigan tarmoq hujumlarini aniqlash va bartaraf etish usul va algoritmlari”** nomli uchinchi veb interfeysga qaratilgan tarmoq hujumlarini aniqlash usuli va algoritmi va tarmoq hujumlarni aniqlashning VITE usuli va algoritmi hamda tarmoq hujumlarini bartaraf etishning modifikatsiyalangan tarmoqlararo ekrani ishlab chiqilgan.

Birinchi paragrafda so‘rovlarning statistik tuzilmasi va veb sahifalarni mantiqiy toifalarini hisobga olgan holda veb-ilovalar so‘rovini tavsiflash uchun ma’lumotlarni vektor formati shakllantirildi. Vektor format asosida veb interfeysga qaratilgan tarmoq hujumlarini aniqlash usuli va algoritmi ishlab chiqilgan.

Veb interfeysga qaratilgan hujumlardan himoyalanish uchun taklif etilayotgan usulning mohiyati quyidagicha:

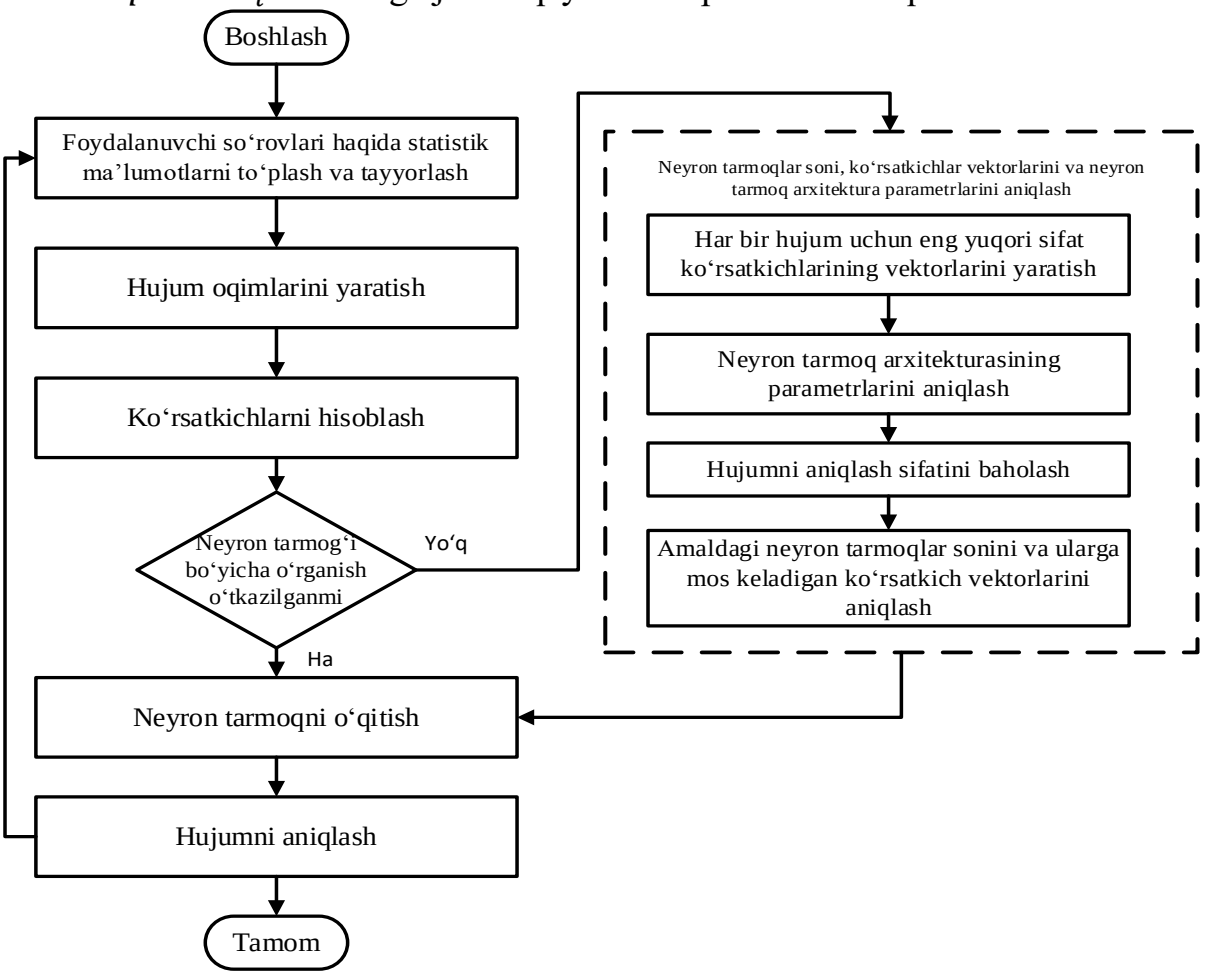
1. Foydalanuvchilar harakatlari to‘g‘risidagi statistik axborotni tayyorlash;
2. Xizmat ko‘rsatishni rad etishga olib keluvchi hujum ta’sirlarini turli toifalari to‘g‘risida statistik axborotni generatsiyalash;
3. Ko‘rsatkichlarni (va statistik tuzilmalarni muvofiq ko‘rsatkichlari) qiymatlarini ko‘rilayotgan vaqt davrida hisoblash;
4. Hujumlarni turli toifalarni aniqlash uchun eng muvofiq ko‘rsatkichlar to‘plamini shakllantirish va ko‘rsatkichlarni qo‘llanishini baholash;
5. Hujumlarni aniqlash sifati va hujumlarni turli toifalari uchun neyron tarmoqlar arxitekturasi eng yaxshi parametrlarini aniqlash;
6. Foydalaniladigan neyron tarmoqlar miqdorini kamaytirish uchun hujum qilinuvchi kuchlar sinflari bo‘yicha hujumni turli toifalarini guruhlash;
7. Neyron tarmoqlarni o‘qitish;
8. Xizmat ko‘rsatishni rad etish toifasidagi hujumlarni aniqlash uchun neyron tarmoqlardan foydalanish;

9. Zarur bo‘lganda yangi statistika asosida neyron tarmoqlarni qayta o‘qitish.

Foydalanuvchilarni veb-ilovalarga so‘rovini tavsiflash uchun quyidagi ma’lumotlarni vektor formati ishlab chiqilgan:

($Time_i$; $SessionID_i$; $IsSessionStart_i$; URL_i; $Parameters_i$; IP_i; $Referer_i$; $UserAgent_i$; $Latency_i$; $DocSize_i$; $Memory_i$; $CpuTime_i$);

- $Time_i$– veb-ilovalardagi so‘rovni seriyali raqami;
- $SessionID_i$ – seans identifikatori;
- $IsSessionStart_i$ – sessiya boshlanish identifikatori;
- URL_i– so‘rovni URL manzili;
- $Parameters_i$- GET-so‘rovi parametrlari;
- IP_i– so‘rov amalga oshirilgan IP manzil;
- $Referer_i$ – oldingi kirilgan sahifa manzili;
- $UserAgent_i$–mijoz dastur identifikator qatori;
- $Latency_i$ –so‘rovi qayta ishlanishida serverni javob vaqti;
- $DocSize_i$ – foydalanuvchi tomonidan so‘rovga javobi yuklangan ma’lumot hajmi;
- $Memory_i$ - so‘rovni qayta ishlash uchun foydalanilayotgan serverni tezkor xotirasi hajmi;
- $CpuTime_i$– so‘rovga javob qaytarishni protsessor vaqti.



2-rasm. Veb-interfeysga qaratilgan xizmat ko‘rsatishni rad etish toifasidagi hujumlarni aniqlash usulining umumiy sxemasi

Veb-interfeysga qaratilgan xizmat ko‘rsatishni rad etish toifasidagi hujumlarni aniqlash algoritmi quyidagi ketma – ketlikda amalga oshiriladi.

Birinchi qadam. Foydalanuvchilarning statik va dinamik so‘rovlarini to‘g‘risidagi ma’lumotlarni to‘plash.

Ikkinchi qadam. Foydalanuvchi so‘rovlari haqida statik ma’lumotlarni hujum oqimlari blokiga uzatish.

Uchinchi qadam. Tizimdagi hujum oqimlarini yaratish.

To‘rtinchi qadam. Hujum oqimlaridagi ko‘rsatgichlarni hisoblash. Ya’ni amalga oshish yoki amalga oshmaslik ehtimolligini hisoblash.

Beshinchi qadam. Neyron tarmoq bo‘yicha tekshirish o‘tkazilganligini tekshirish.

Oltinchi qadam. Neyron tarmoqni o‘qitish. Bunda neyron tarmoqni o‘qituvchi yordamida o‘qitish asosida har bir hujumning eng yuqori sifat ko‘rsatgichlari vektorlarini yaratib olish va neyron tarmoq arxitekturasining parametrlarini aniqlash hamda hujumni aniqlash sifitini baholashni amalga oshirish vazifalari bajariladi.

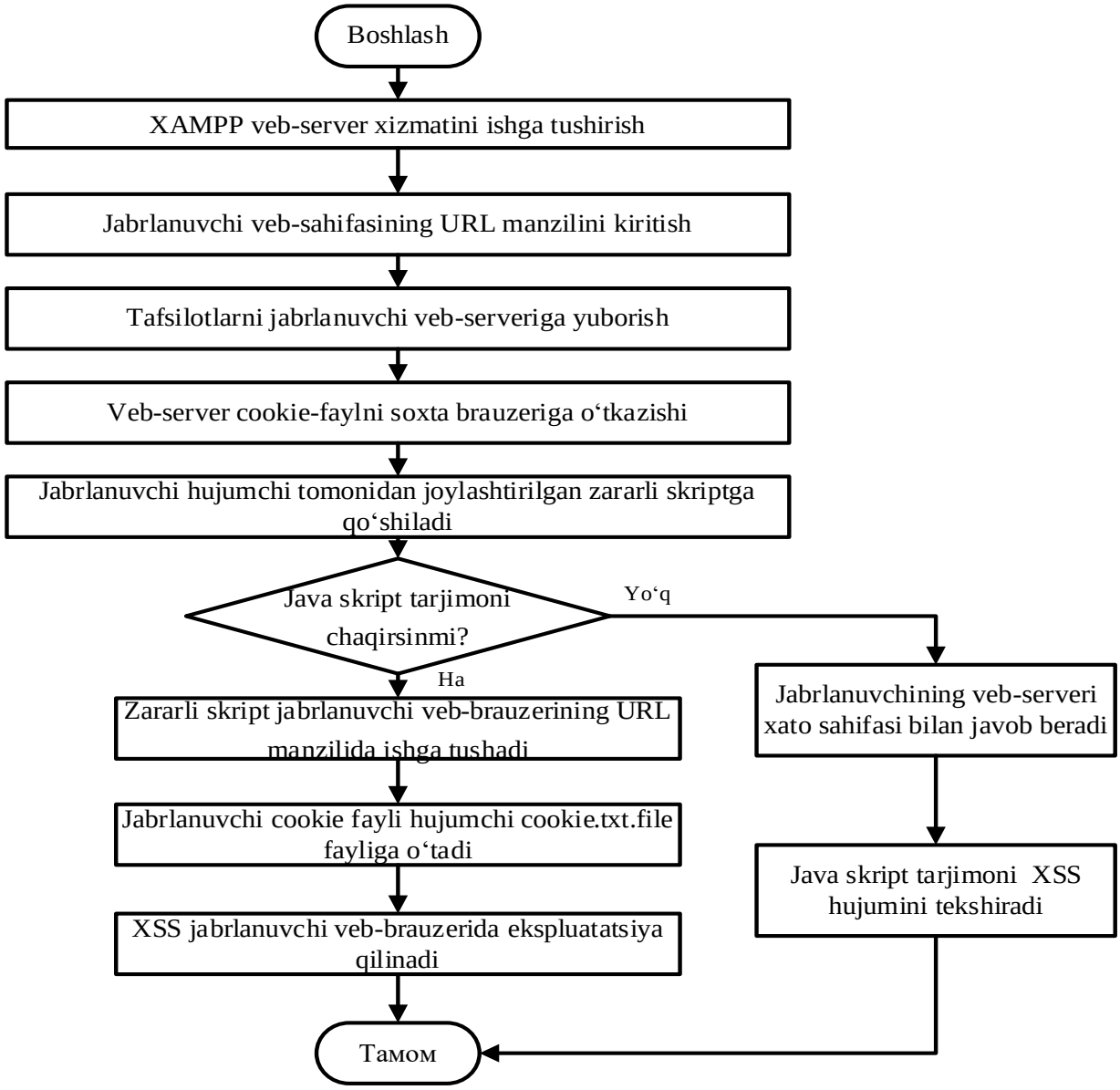
Yettinchi qadam. Hujumni aniqlash.

Ikkinchi paragrafda Veb serverga bo‘ladigan tarmoq hujumlarini xavfsiz holatga keltiradigan muhitda ishlaydigan cheklangan muhit hosil qilish natijasida tarmoq hujumlarini aniqlashning VITE usuli va algoritmi ishlab chiqilgan. Natijada veb serverga qaratilgan tarmoq hujumlarni amalga oshirish imkonini beradigan platformalar xususiyatlaridan foydalanib, foydalanuvchining shaxsiy ma’lumotlarini (cookie fayllari, sessiya identifikatorlari va boshqalar) o‘g‘irlashdan himoyalash mumkin bo‘ldi.

Kibermakondagi jinoiy ishlar soni yiliga ko‘payib boradi. OWASP top 10 ga asoslangan ma’lumotlarga ko‘ra, tashkilotlar tomonidan o‘tkazilgan so‘nggi ikki yil ichidagi so‘rovlar natijasiga ko‘ra, eng keng tarqalgan hujumlar SQL, NoSQL, OS va LDAP kabi inyeksiyaga asoslangan hujumlardir. Whitehat Security ma’lumotlariga ko‘ra 83 foizi saytda kamida ikkita zaiflik mavjudligi e’lon qilingan. Bu zaifliklarni aniqlash uchun biz usul taklif etdik. Veb saytlarni himoyalashda foydalaniladigan tarmoqlararo ekran veb ilovalarni bir vaqtda bir nechtasini nazoratga olishi kerakligidan kelib chiqib usul VITE (Veb ilovalar tarmoqlararo ekrani) deb nomlandi.

Usul uch bosqichda amalga oshiriladi. Bular tahlil qilish, aniqlash va oldini olish ya’ni bartaraf etish. Tahlil qilish bosqichi uchun amalda foydalanib kelinayotgan intellektual usullardan foydalanish maqsadga muvofiq, chunki bu usullarni samaradorligi juda yuqori ekanligi bir nechta ilmiy ishlarda asoslangan va isbotlangan. Asosiy kiritilayotgan yangilik aniqlash va oldini olish bosqichida amalga oshiriladi.

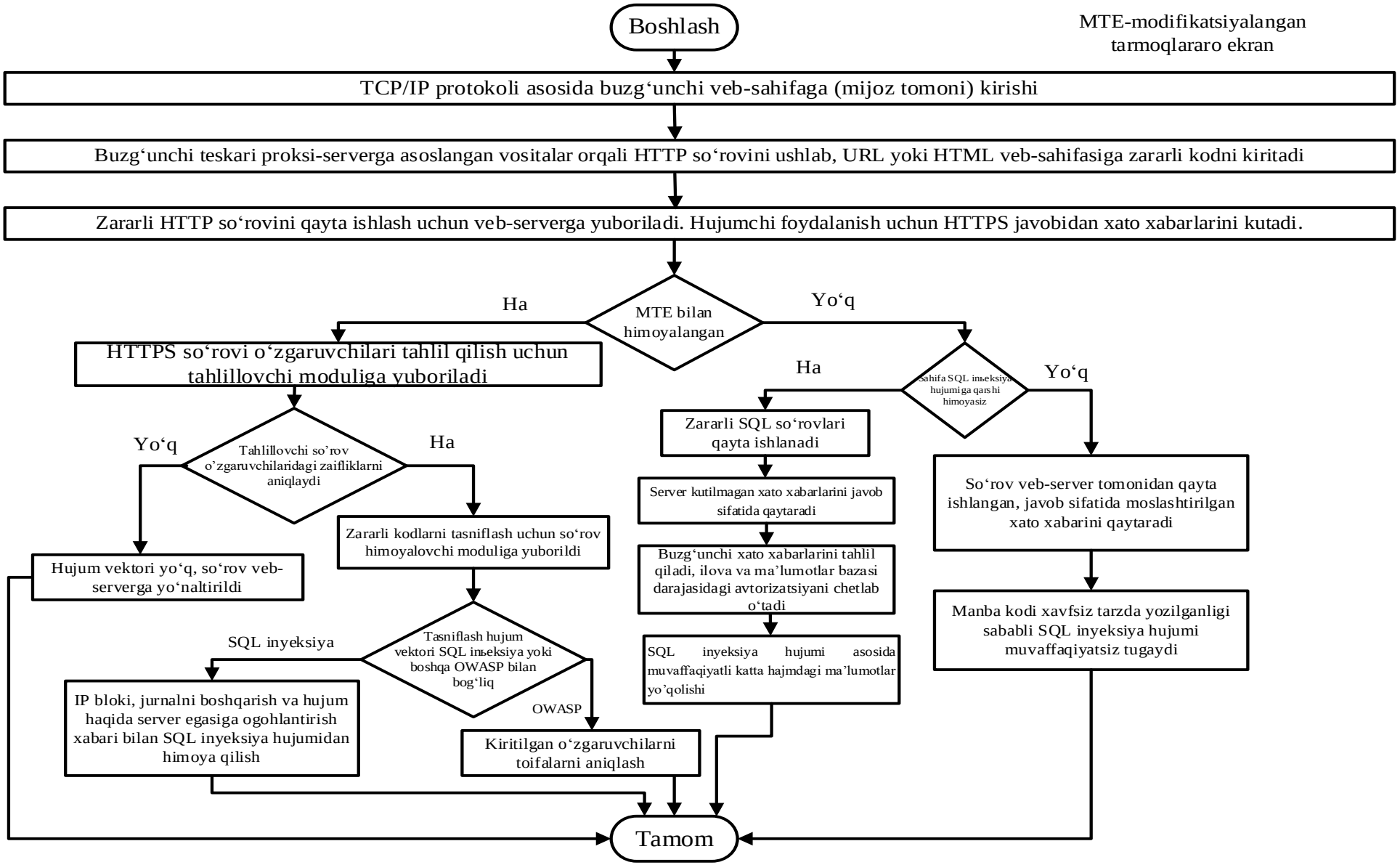
Uchinchi paragrafda Veb-ilovalardagi zaifliklarni topish, yangi hujum vektorlarini aniqlash, SQL inyeksiya hujum vektorlarining turlarini tahlil qilish va veb-ilovalarni OWASP hujum vektorlaridan himoya qilish uchun TCP/IP protokoli darajasida ishlaydigan va bulutli ma’lumotlar markazlarida joylashtirilgan veb-ilovalarning zamonaviy himoyasini tashkil etish asosida modifikatsiyalangan tarmoqlararo ekrani taklif etilgan.



3-rasm. LocalHost serverida XSS hujumi aniqlash algoritmining blok-sxemasi

Taklif etilayotgan modifikatsiyalangan tarmoqlararo ekran ish rejimi va ishlash mexanizmi quyidagi ketma ketlikda amalga oshiriladi. Buning uchun eng ko‘p uchragan SQL inyeksiya hujumini amalga oshirish zarur. Bu usul oddiy xatoga asoslangan SQL inyeksiyadir. Bunda buzg‘unchilar kutilmagan buyruqlar kiritadilar, ya’ni so‘rov parametrlariga noto‘g‘ri kirish, masalan, o‘rtadagi odam hujumi, ba’zi vositalar yordamida so‘rov o‘zgaruvchilarini to‘xtatish.

SQL inyeksiya	**So‘rov kontentlari/ hujum vektorlari kalit so‘zlari**
Xatolikka asoslangan	‘ i.e. extra quote in SQL statement
	SELECT,CONCAT,@@VERSION Avoid all special characters in SQL statement , =!@#$%^&*()+-_={}[]:;”’
Birlashmaga asoslangan	‘ ,UNION SELECT ;-- @@version Ex. id =1’ UNION SELECT 1;--
Mantiqiy qiymatlarga asoslangan	’, and ,union ,select ,;-- ,substring, length Ex. 1’ and 1=1 UNION select 1;-- Ex. Substring(@@version,2,1)=1;-- Ex. length(database())==3;--
Vaqtga asoslangan	Sleep();--Ex. 1’ and sleep(10);--



4-rasm. Tarmoq hujumlarni bartaraf etishning modifikatsiyalangan tarmoqlararo ekranining ishlash sxemasi

SQL inyeksiya hujumlarining turli vektorlarini o‘rganishdan so‘ng, veb-sahifalardagi zaifliklardan foydalanishga urinayotgan kontent deb ataydigan muayyan asosiy parametrlar aniqlanadi. Agar bunday hujum vektorlari veb-ilovalar tarmoqlararo ekrani tomonidan kontentni tahlil qilish orqali rad etilsa, buzg‘unchilar hech qachon ilovalar va ma’lumotlar bazasi serveriga kira olmaydi va bu dastur xavfsizligi sohasida katta samaradorlikka ega bo‘ladi. Buning uchun taklif etilgan tarmoqlararo ekranning natijaviy tarmoq kontent siyosati quyidagicha amalga oshiriladi.

Tarmoq hujumlarini bartaraf etishning modifikatsiyalangan tarmoqlararo ekranini ishlashining qadamli algoritmi quyidagi ketma ketlikda amalga oshiriladi.

Birinchi qadam. TCP/IP protokoli asosida buzg‘unchi veb-sahifaga (mijoz tomoni) kirishi tahlil qilish.

Ikkinchi qadam. Buzg‘unchi teskari proksi-serverga asoslangan vositalar orqali yuborgan HTTP so‘rovini ushlab, URL yoki HTML veb-sahifasida zararli kod mavjudligini tekshirish.

Uchinchi qadam. Aniqlangan zararli HTTP so‘rovini qayta ishlash uchun veb-serverga yuborish. HTTPS so‘rovi o‘zgaruvchilarini tahlil qilish hamda tahlillovchi so‘rov o‘zgaruvchilardagi zaifliklarni aniqlash.

To‘rtinchi qadam. Hujum vektori yo‘q bo‘lgan holda so‘rovni veb serverga yo‘naltirish aks holda zararli kodlarni tasniflash uchun so‘rov himoyalovchi moduliga yuborish.

Beshinchi qadam. Tasniflash hujum vektori SQL inyeksiya yoki boshqa OWASP bilan bog‘liqligini tekshirish. Agar OWASP bilan bog‘liqligi bo‘lsa kiritilgan o‘zgaruvchilarni toifalarni aniqlash.

Oltinchi qadam. IP bloki, jurnalni boshqarish va hujum haqida server egasiga ogohlantirish xabari bilan SQL inyeksiya hujumidan himoya qilish xabarini yuborish.

Yettinchi qadam. Buzg‘unchi tomonidan yuborilgan xato xabarlarini tahlil qilish, ilova va ma’lumotlar bazasi darajasidagi avtorizatsiyani chetlab o‘tganligini tekshirish.

Sakkizinchi qadam. So‘rovni veb-server tomonidan qayta ishlab, javob sifatida moslashtirilgan xato xabarini qaytarish.

To‘qqizinchi qadam. Tugatish.

Dissertatsiyaning **“Tarmoq hujumlarini aniqlash jarayoni samaradorligini baholash va amaliyotga tatbiq etish natijalari”** nomli to‘rtinchi bobida zaifliklarni va tarmoq hujumlarini aniqlash usullarining samaradorligini baholash hamda tarmoq hujumlarini aniqlashni dasturiy vositasining funksional strukturasi va ishlash prinsipi hamda joriy etishdan olingan tajriba-hisoblash natijalari keltirilgan.

Birinchi paragrafda zaifliklarni va tarmoq hujumlarini aniqlash usullarining samaradorligini baholash amalga oshirilgan.

Zaifliklarni va tarmoq hujumlarini aniqlash hamda axborot xavfsizligini ta’minlash samaradorligini oshirish bo‘yicha Kiberxavfsizlik markazi tomonidan bir qancha tavsiyalar keltirib o‘tilgan. Bular:

1. Litsenziya va sertifikatga ega operatsion tizimlar va dasturlardan foydalanish.

2. Amaldagi operatsion tizimlar, dasturiy ta’minot va xavfsizlik komponentlarining so‘nggi versiyalarini muntazam yangilab turish. Yangilash ishlarini rasmiy manbalardan amalga oshirilish.

3. Kelgusida zararli dasturlarni qidirish, o‘chirib tashlash va ulardan himoya qilish funksiyalariga ega xavfsizlik plaginlaridan foydalanish.

4. Muntazam ravishda ma’lumotlar bazalari, fayllar, pochta va hokazolarni zaxiralash ishlarni amalga oshirish.

5. Foydalanilmayotgan plaginlarni o‘chirib tashlash.

6. Parol asosidagi autentifikatsiyasini kuchaytirish.

7. Yangilangan virus bazalariga ega antivirus dasturlari o‘rnatilgan qurilmalardan (kompyuterlar, planshetlar) axborot tizimiga yoki veb-saytga kirishni ta’minlash.

8. Axborot tizimlari va resurslarini axborot xafsizligi talablariga muvofiqligi bo‘yicha ekspertizalarni o‘tkazish. Ekspertiza natijalari bo‘yicha yuborilgan tavsiyalar asosida aniqlangan zaifliklarni o‘z vaqtida bartaraf etish.

9. Foydalanuvchilar (xodimlar)ning axborot-kommunikatsiya texnologiyalari va axborot xavfsizligi sohasidagi malakasi va bilim darajasini muntazam oshirib borish.

10.Kiberxavfsizlik hodisalarining tahdidlarini va oqibatlarini bartaraf etish uchun tezkor aniqlash va tegishli choralarni ko‘rish.

1-jadval

Serverlardagi zaifliklarni aniqlashning uch bosqichli testlash usulining testlash natijalari.

Bunda: Inyeksiya zaifliklar (IZ), biznes mantiq zaifliklari (BMZ), seans boshqaruvidagi zaifliklar (SBZ).

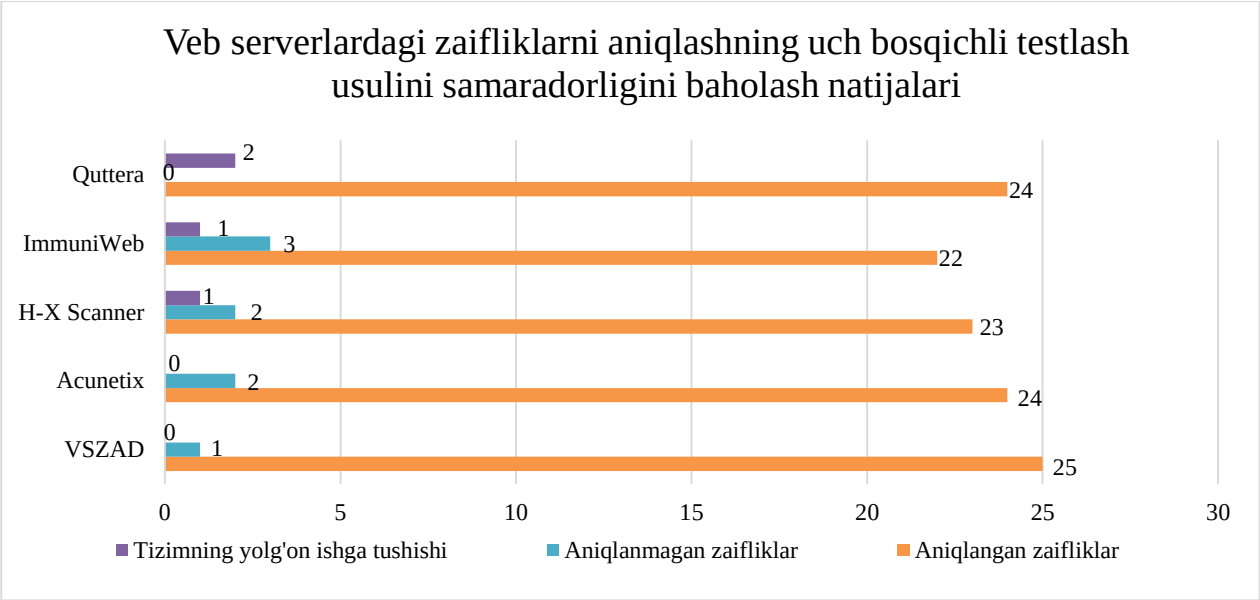
Zaifliklar turlari	Jami zaifliklar soni	Aniqlangan zaifliklarlar	Aniqlanmagan zaifliklarlar	Tizimni yolg‘on ishga tushishlari
IZ	23	22	0	1
BMZ	11	10	1	0
SBZ	16	15	1	0

2-jadval

Veb serverlardagi zaifliklarni aniqlashning uch bosqichli testlash usulini samaradorligini baholash natijalari

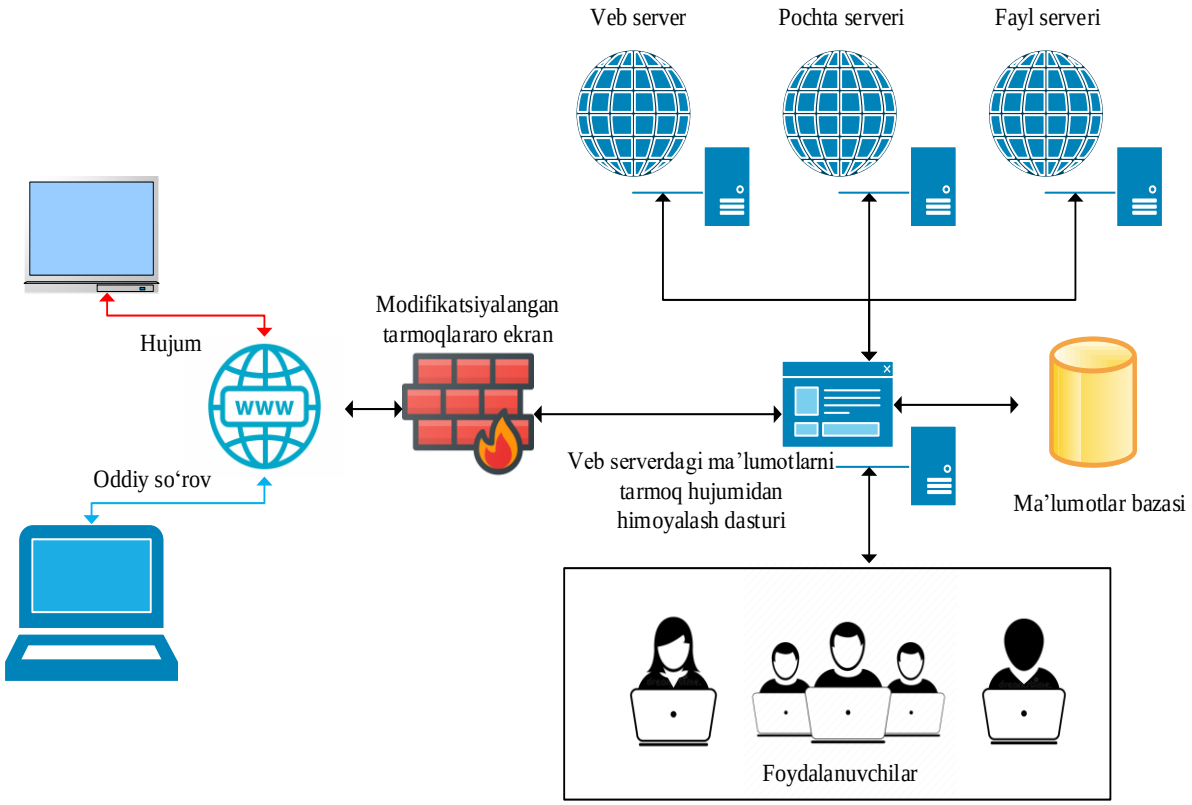
Bunda veb serverdagi zaifliklarni aniqlash dasturi (VSZAD).

Zaifliklarni aniqlash dasturlari	Jami zaifliklar	Aniqlangan zaifliklar	Aniqlanmagan zaifliklar	Tizimni yolg‘on ishga tushishlari
VSZAD	26	25	1	0
Acunetix	26	24	2	0
H-X Scanner	26	23	2	1
ImmuniWeb	26	22	3	1
Quttera	26	24	0	2



5 – rasm. Veb serverlardagi zaifliklarni aniqlashning uch bosqichli testlash usulini samaradorligini baholash natijalari

Ikkinchi paragrafda tarmoq hujumlarini aniqlashni dasturiy vositasining funksional strukturasi (6-rasm).



6-rasm. Veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoya qilish dasturiy vositasining funksional strukturasi

Dasturiy vosita proksi-server sifatida ishlaydi, ammo ma’lum bir server sertifikatini tekshirish orqali HTTPS trafigini o‘rganish imkoniyati natijasida qo‘shimcha funksiyalarni ham bajaradi. Bular:

- veb serverdagi so‘rovlar hajmini muvozanatlash va nazoratlash;
- SSL trafigini to‘xtatish va shu kabi boshqa funksiyalardir.

Ishlab chiqilgan dasturiy vosita veb serverga quyidagi tarzda ulanishni amalga oshiradi:

- SPAN porti bilan real vaqtda tarmoq monitoringi rejimida.
- proksi rejimi: shaffof, ko‘prik va teskari rejimda.

Uchinchi paragrafda tashkilot veb serverdagi zaifliklarni aniqlash dasturiy vositasini amaliyotga tatbiq etish natijalari keltirilgan.

Veb serverdagi ochiq portlar va ulardagi zaifliklarni aniqlash va veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoyalash dasturiy vositasi “Kiberxavfsizlik markazi” davlat unitar korxonasida, “UZINFOCOM Davlat axborot tizimlarini yaratish va qo‘llab-quvvatlash bo‘yicha yagona integrator” ma’suliyati cheklangan jamiyatida va “MAXSUS XIZMAT BUX” ma’suliyati cheklangan jamiyatida joriy etilgan va natijalar quyida keltirilgan.

“Kiberxavfsizlik markazi” davlat unitar korxonasida veb serverdagi ochiq portlar va ulardagi zaifliklarni aniqlash va veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoyalash uchun ishlab chiqilgan dasturiy vosita 152348 ta tarmoq hujumlarnini 98.7% aniqlik va 1.3% xatolik qayd etgan holda aniqlash imkonini berdi. Sinovdan o‘tish jarayonida xatoliklar haqida tizim administratorini ogohlantirish funksiyasi real vaqt rejimida ishlashi tasdiqlandi.

“UZINFOCOM Davlat axborot tizimlarini yaratish va qo‘llab-quvvatlash bo‘yicha yagona integrator” ma’suliyati cheklangan jamiyatida veb serverdagi ochiq portlar va ulardagi zaifliklarni aniqlash va veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoyalash maqsadida tajribaviy sinovdan o‘tkazildi. Sinov natijasida ishlab chiqilgan dasturiy vosita veb serverdagi 153 ta ochiq portni va 6 turdagi zaifliklarni hamda 163469 ta tarmoq hujumlarini 97.9% aniqlik va 2.1% xatolik qayd etgan holda aniqlash imkonini berdi. Olingan natijalar asosida shuni aytish mumkinki, ushbu dasturiy vositadan foydalanish bir vaqtning o‘zida veb serverdagi ochiq portlarni va zaifliklarni hamda tarmoq hujumlarini aniqlash imkonini beradi.

“MAXSUS XIZMAT BUX” ma’suliyati cheklangan jamiyatida veb serverdagi ochiq portlar va ulardagi zaifliklarni aniqlash va veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoyalash maqsadida sinovdan o‘tkazildi. Sinov natijasida ishlab chiqilgan dasturiy vosita veb serverdagi 148 ta ochiq portni va 6 turdagi zaifliklarni hamda 135238 ta tarmoq hujumlarini 97.5% aniqlik va 2.5% xatolik qayd etgan holda aniqlash imkonini berdi. Sinov natijalari shuni ko‘rsatdiki, ushbu dasturiy vositadan foydalanish bir vaqtning o‘zida veb serverdagi ochiq portlarni va zaifliklarni hamda tarmoq hujumlarini samarali aniqlash imkonini beradi.

XULOSA

“Veb-serverlardagi axborotni tarmoq hujumlaridan himoyalash usullari va algoritmlari” mavzusidagi dissertatsiya ishi bo‘yicha olib borilgan tadqiqotlar natijasida quyidagi xulosalar taqdim etildi:

1 US-CERT, Open Information Security Foundation tashkiloti tomonidan shakllantirilgan statistik ma’lumotlar asosida dasturiy mahsulot ishlab chiquvchilarning dasturlaridagi zaifliklarini bitta identifikator tizimida (masalan, CVE-ID) guruhlaydigan veb serverlardagi zaifliklarni reyestri shakllantirildi.

Natijada veb serverlardagi zaifliklar va ular asosida amalga oshiriladigan hujum turlarini OWASP ning zaifliklar bazasiga integratsiya qilish imkonini berdi.

2 Uch sinfdan iborat veb ilovalarni testlash usuli ekvivalentlik testini 4 ta bosqichda, chegara testini 9 bosqichda va qarorlar jadvali testini 5 ta bosqichda amalga oshirish asosida veb serverlardagi ilovalarni ekvivalentlik, chegara va qarorlar jadvali asosida testlashga natijalariga ko‘ra veb serverlardagi zaifliklarni aniqlashning uch bosqichli testlash usuli ishlab chiqilgan. Natijada veb server va ilovalardagi zaifliklarni aniqlash uchun har xil turdagi ma’lumotlar to‘plamiga to‘liq kirish imkonini berdi.

3 Aloqa kanali, protokoli, www server ishlaydigan apparat platformasi va operatsion tizimi hamda veb server ma’lumotlar bazasini boshqarish tizimidagi va shu kabi zaifliklarni asosiy uchta katta guruhlarga ajratib olish hamda ushbu guruhlarga kiradigan zaifliklarni ma’lum ketma-ketliklar asosida umumlashgan guruhlarini yaratish imkonini beradigan veb serverlardagi zaifliklarni guruhlash usuli va algoritmi ishlab chiqildi. Natijada har bir zaiflik asosida amalga oshiriladigan hujum uchun himoya mexanizmi emas balki zaifliklarni guruhiga tegishli bo‘lgan hujumlar himoya mexanizmi ishlab chiqish imkonini bergan.

4 So‘rovlarning statistik tuzilmasi va veb sahifalarni mantiqiy toifalarini hisobga olgan holda veb-ilovalar so‘rovini tavsiflash uchun ma’lumotlarni vektor formati shakllantirildi. Vektor format asosida veb interfeysga qaratilgan hujumlarni aniqlash usuli va algoritmi ishlab chiqildi. Natijada veb interfeysga qaratilgan hujum so‘rovlarini ma’lumotlar bazasiga ruxsatsiz o‘tishdan himoyalash imkonini berdi.

5 Xavfsiz muhit yaratishga imkon beradigan cheklangan muhit asosida veb serverga bo‘ladigan tarmoq hujumlarini aniqlashning VITE usuli va algoritmi ishlab chiqilgan. Natijada veb serverga qaratilgan tarmoq hujumlarini amalga oshirish imkonini beradigan platformalar xususiyatlaridan foydalanib, foydalanuvchining shaxsiy ma’lumotlarini (cookie fayllari, sessiya identifikatorlari va boshqalar) o‘g‘irlashdan himoyalash imkoniga ega bo‘lindi.

6 Zaifliklarni aniqlashning uch bosqichli testlash usuli va tarmoq hujumlarni aniqlashning VITE usullari asosida ishlab chiqilgan veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoyalashning dasturiy vositasi zaifliklarni 96,1% aniqlikda, hujumlarni esa 97,9% aniqlikda aniqlash imkonini berdi. Zaifliklarni aniqlashda bundanda yaxshiroq samaradorlik ko‘rsatgichiga erishish bo‘yicha tavsiyalar keltirildi.

Taklif etilgan usullar asosida ishlab chiqilgan veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoyalashning dasturiy vositasi korxona va tashkilotlardagi veb server va ilovalarni himoyalash uchun foydalaniladigan axborot xavfsizligini ta’minlash tizimlarining samaradorligini ortishi va veb ilovalarning foydalanuvchanligini saqlab qolish imkonini beradi.

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

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ИБРОХИМОВ АЗИЗБЕК РАВШАНБЕК УГЛИ

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ВЕБ-СЕРВЕРАХ ОТ СЕТЕВЫХ АТАК

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ

Ташкент-2024

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, Науки и Инноваций Республики Узбекистан за № B2023.3.PhD/T4056.

Диссертация выполнена в Ташкентском университете информационных технологий.

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

Научный руководитель:	**Хамдамов Рустам Хамдамович** доктор технических наук, профессор
Официальные оппоненты:	**Жураев Гайрат Умарович** доктор физико-математических наук, доцент
	Насруллаев Нурбек Бахтиёрович доктор философии технических наук, доцент
Ведущая организация:	**ООО «UNICON.UZ» - Центр научно-технических маркетинговых исследований**

Защита диссертации состоится «14» января 2024 года в 11[30] 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 №155). (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43).

Автореферат диссертации разослан «12» января 2024 года.
(протокол рассылки № 4 от «11» января 2024 года.)

Б.Ш. Махкамов
Председатель научного совета по присуждению ученых степеней, д.э.н., профессор

М.С.Санткамолов
Ученый секретарь научного совета по присуждению ученых степеней, д.э.н., доцент

С.К. Ганиев
Председатель научного семинара при научном совете по присуждению ученых степеней, д.т.н., профессор

ВВЕДЕНИЕ (аннотация к диссертации доктора философии (PhD))

Актуальность и необходимость темы диссертации. Для предприятий и организаций, находящихся в любой точке мира, при осуществлении международных рыночных отношений считается достаточным наличие доступа в интернет на территории их расположения. Официальные веб-страницы являются, своего рода, «лицом» предприятий и организаций на международной и национальной арене.) Вот почему количество атак, направленных на веб-серверы и веб-приложения, растет день ото дня. По данным компании “Kaspersky” количество атак на веб-сервер резко возросло: за последний год было обнаружено 687 861 449 атак, причем основная их часть пришлась на 10 стран[3]. Среди них такие зарубежные страны, как Чехия, США, Германия, Нидерланды, Франция, Российская Федерация и другие. В этих, а также и в других странах важное значение приобретает разработка методов и алгоритмов защиты информации на веб-серверах от сетевых атак, а также совершенствование систем защиты веб-серверов организаций.

В мире ведутся исследования и разработки, направленные на совершенствование методов и алгоритмов защиты информации на веб-серверах от сетевых атак, а также на обнаружение атак с помощью нейронных сетей. Одной из важных задач в этом плане является разработка методов обнаружения сетевых атак, в том числе нацеленных на веб-интерфейс. Однако, поскольку не существует единого решения для обнаружения всех багов на веб-сервере, становится необходимым разработать механизм защиты с использованием современных методов для обнаружения открытых портов и уязвимостей на веб-сервере.

В нашей республике в органах государственного и хозяйственного управления реализуется комплекс мер по защите от атак, направленных на веб-сервер.

В Указе Президента Республики Узбекистан «О Стратегии развития Нового Узбекистана на 2022-2026 годы[4]» определен ряд задач, направленных на защиту информации, в том числе пункт 327 89-цели: «Дальнейшее укрепление прав граждан в области свободы получения и распространения информации» раздела VII. «Укрепление безопасности и оборонного потенциала страны, ведение открытой, прагматичной и активной внешней политики»: «...определение основных направлений обеспечения кибербезопасности интернет-пространства доменной зоны «UZ» и комплексных задач по защите систем электронного правительства, энергетики, цифровой экономики и других направлений, касающихся важной информационной инфраструктуры». Одними из важных вопросов при реализации данных задач являются применение современных методов защиты информации на веб-серверах от сетевых атак и использование новых систем защиты веб-сервера.

---

[3] https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_rus.pdf

[4] Указ Президента Республики Узбекистан от 28 января 2022 года № УП-60 «О Стратегии развития Нового Узбекистана на 2022-2026 годы»

Данное диссертационное исследование, в определенной степени, служит выполнению задач, предусмотренных в Указе Президента Республики Узбекистан №УП-60 «О Стратегии развития Нового Узбекистана на 2022 - 2026 годы» от 28 января 2022 года, в Указе Президента Республики Узбекистан №УП-5349 «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций» от 19 февраля 2018 года, в Постановлении Президента Республики Узбекистан №ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» от 21 ноября 2018 года, в Постановлении Президента Республики Узбекистан №ПП-4452 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» от 14 сентября 2019 года и в других нормативно-правовых актах, касающихся данной деятельности.

Соответствие исследования приоритетным направлениям развития науки и технологий республики.

Данное исследование выполнено в соответствии с приоритетными направлениями развития науки и технологий республики IV. «Развитие информатизации и информационно-коммуникационных технологий»

Степень изученности проблемы. Научному исследованию методов выявления уязвимостей при обеспечении безопасности веб-сервера и приложений, а также практическому применению разработанных методов и алгоритмов обнаружения открытых портов и уязвимостей на веб-сервере с применением современных методов посвящены многочисленные работы таких зарубежных учёных, как: А. Стасюк, А. Корченко, М. Саттон, А. Грин, П. Амини, М.В. Щерба, Д.Е. Гамаюнов, И.С. Александров и других. Ряд научных исследований по применению метода группирования при защите информации на веб-серверах от сетевых атак были проведены Крисом Скиннер, Ш.Харрисом, А.Антоновым, Брайаном Кребс, Саталином Симпану. Кроме того, такими организациями, как Tadviser, OWASP, Kaspersky проводятся инженерно-исследовательские работы по разработке программно-аппаратных средств защиты информации на веб-серверах от сетевых атак с применением современных методов.

В Узбекистане научные исследования по разработке методов и алгоритмов защиты информации на веб-серверах от сетевых атак велись академиком Т.Ф. Бекмуратовым и в настоящее время научные исследования проводятся научными коллективами под руководством С.К. Ганиева, Р.Х. Хамдамова, М.М. Каримова и другими.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование было выполнено в рамках научно-исследовательских работ по проекту 598661-EPP-1-2018-1-RO-EPPKA2-CBHE-JP “Developing Services for Individuals with Disabilities” в Ташкентском университете информационных технологий имени Мухаммада ал-Хоразмий.

Целью исследования является разработка методов и алгоритмов защиты информации от сетевых атак, позволяющих повысить эффективность системы защиты веб-сервера.

Задачи исследования:

сравнительный анализ методов защиты информации на веб-серверах от сетевых атак и разработка структуры системы обнаружения уязвимостей;

разработка метода трехэтапного тестирования для обнаружения уязвимостей на веб-серверах;

разработка метода и алгоритма группирования уязвимостей на веб-серверах;

разработка метода и алгоритма обнаружения сетевых атак, нацеленных на веб-интерфейс.

В качестве **объекта исследования** был определен процесс обнаружения уязвимостей на веб-сервере и защиты информации от сетевых атак.

Предметом исследования являются методы и алгоритмы обнаружения уязвимостей на веб-сервере и защиты информации от сетевых атак.

Методы исследования. В рамках данного исследования использовались нейронные сети, теория вероятностей, теория векторных графов, дискретная математика и методы объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

на основе собранной международными организациями базы данных известных на данный момент уязвимостей информационной безопасности сформирован реестр уязвимостей веб-серверов, группирующий уязвимости веб-серверов по среде их существования через единую систему идентификаторов;

разработан трехэтапный метод тестирования для выявления уязвимостей в приложениях, основанный на тестировании приложений на веб-серверах в режиме реального времени на основе сочетания тестов эквивалентности, пороговых значений и таблицы решений;

на основе создания обобщенной группы параметров веб-сервера по каналу связи, протоколу и среде аппаратной платформы, имеющейся на веб-сервере, разработан метод и алгоритм группирования уязвимостей в веб-серверах, соответствующих каждому уровню параметров;

на основе статистической структуры запросов, направляемых на веб-сервер, и логических категорий веб-страниц разработаны метод и алгоритм обнаружения сетевых атак, направленных на веб-интерфейс, на основе векторного формата запроса;

разработаны метод и алгоритм VITE для обнаружения сетевых атак на основе протокола, работающего на уровне уязвимостей в результате защиты сетевых атак на веб-сервер на основе обобщенных групп параметров веб-сервера.

Практические результаты исследования заключаются в следующем:

разработано программное средство защиты информации от сетевых атак, основанное на обнаружении уязвимостей на веб-сервере;

на основе организации современной защиты веб-приложений усовершенствован межсетевой экран для обнаружения уязвимостей в веб-приложениях и защиты веб-приложений от векторов атак, который работает на уровне протокола TCP/IP.

Достоверность результатов исследования. Достоверность результатов исследования объясняется результатами реального и экспериментального анализа, полученными в различных условиях методами обнаружения сетевых атак, методами обнаружения сетевых атак, нацеленных на веб-интерфейс, методами обнаружения и группирования уязвимостей на веб-серверах.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования объясняется разработанными методом и алгоритмом этапов обнаружения уязвимостей на веб-серверах, разработкой метода трехэтапного тестирования и алгоритма обнаружения уязвимостей на веб-серверах, методом и алгоритмом обнаружения сетевых атак нацеленных на веб-интерфейс, а также методом и алгоритмом обнаружения сетевых атак VITE.

Практическая значимость результатов исследования объясняется тем, что разработанное на основе предложенных методов и алгоритмов программное средство способствует повышению эффективности процесса выявления уязвимостей на веб-сервере организации и защиты информации от сетевых атак.

Внедрение результатов исследования. На основе полученных научных результатов по методам и алгоритмам, а также программному средству защиты информации на веб-сервере от сетевых атак:

разработанное программное средство на основе методов и алгоритмов защиты информации на веб-сервере от сетевых атак внедрено в практическую деятельность Государственного унитарного предприятия «Центр кибербезопасности» (Справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан № 33-8/6723 от 11 октября 2022 года). Результаты научного исследования позволили обнаружить 152348 сетевых атак в корпоративной сети с точностью 98,7% и ошибкой 1,3%;

разработанное программное средство на основе методов и алгоритмов защиты информации на веб-сервере от сетевых атак внедрено в практическую деятельность общества с ограниченной ответственностью «UZINFOCOM Единый интегратор по созданию и поддержке государственных информационных систем» (Справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан № 33-8/6723 от 11 октября 2022 года). Использование результатов научного исследования позволило выявить 153 открытых порта и 6 типов уязвимостей на веб-сервере организации, а также 163469 сетевых атак с точностью 97,9% и регистрацией ошибок 2,1%;

разработанное программное средство на основе методов и алгоритмов защиты информации на веб-сервере от сетевых атак внедрено в практическую деятельность общества с ограниченной ответственностью «MAXSUS

XIZMAT BUX» (Справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан № 33-8/6723 от 11 октября 2022 года). Использование результатов научного исследования позволило обнаружить 148 открытых портов и 6 типов уязвимостей на веб-сервере организации, а также 135238 сетевых атак с точностью 97.5% и регистрацией ошибок 2.5%.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 2 международных и 2 республиканских научно-практических конференциях.

Опубликованность результатов исследования. Всего по теме диссертации опубликовано 18 научных работ, в том числе 6 статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов докторских диссертаций, из них 3 в зарубежных и 3 в республиканских журналах, а также получены 3 свидетельства об официальной регистрации программы для ЭВМ.

Структура и объем диссертации. Структура диссертации состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет - 115 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и необходимость темы диссертации, приводится соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, определены цели и задачи исследования, объект и предмет исследования, обоснована достоверность полученных результатов, их теоретическая и практическая значимость, состояние практического внедрения результатов исследования, привидены сведения об опубликованности результатов и структуре диссертации.

В первой главе диссертации «**Анализ типов сетевых атак на информацию на веб-серверах и способы защиты от них»**, представлены типы сетевых атак на информацию на веб-серверах, их различия, а также анализ методов обнаружения уязвимостей на веб-серверах и сравнительный анализ методов защиты информации на веб-серверах от сетевых атак.

В первом параграфе проанализированы распределение источников веб-атак по странам, а также пользователи из первых 10 стран по типам сетевых атак на информацию на веб-серверах и объектам, на которые нацелены угрозы безопасности, влияющие на информацию, а также по доле пользователей, подвергшихся атаке.

Во втором параграфе представлен сравнительный анализ преимуществ и недостатков методов обнаружения уязвимостей веб-сервера, приведены сведения о том, кем выполняются методы тестирования, используемые для обнаружения уязвимостей, приведены необходимые знания программирования и реализации, а также основной источник тестовых примеров. По результатам сравнительного анализа эффективность метода черного ящика оказалась высокой.

В третьем параграфе с целью выявления преимуществ и недостатков методов защиты информации на веб-серверах от сетевых атак они разделены на две группы: методы обнаружения сетевых атак на уровне хоста и методы обнаружения сетевых атак на уровне сети. Поскольку видимость данных на 7 уровнях модели OSI становится все более важной при реализации сетевых атак на сетевом уровне, для двух групп был проведен отдельный сравнительный анализ. В результате сравнительного анализа была выявлена высокая эффективность методов обнаружения сетевых атак на сетевом уровне.

Во второй главе диссертации «**Методы и алгоритмы обнаружения и группирования уязвимостей на веб-серверах**» разработаны практически используемые и современные структуры системы обнаружения уязвимостей на веб-серверах, метод и алгоритм этапов обнаружения уязвимостей на веб-серверах, а также метод и алгоритм группирования уязвимостей на веб-серверах.

В первом параграфе данной главы сформирован реестр уязвимостей на веб-серверах на основе статистических данных, сформулированных организацией US-CERT, Open Information Security Foundation, который группирует уязвимости разработчиков программного продукта в одну систему идентификации (например, CVE-ID), а также разработана современная структура системы обнаружения существующих уязвимостей на веб-серверах. В результате уязвимости на веб-серверах и типы атак, на которых они основаны, были интегрированы в базу данных уязвимостей OWASP.

Во втором параграфе разработан метод трехэтапного тестирования на основе реализации теста эквивалентности в 4 этапа, порогового теста в 9 этапов и теста таблицы решений в 5 этапов, то есть метод тестирования веб-приложений, состоящий из трех классов и алгоритм обнаружения уязвимостей на веб-серверах. Метод трехэтапного тестирования позволяет не только выявлять уязвимости, но и устраняет их, обеспечивая защиту информации, а также своевременное обслуживание приложений на веб-серверах.

В третьем параграфе разработан метод и алгоритм группирования уязвимостей в канале связи, протоколе, аппаратной платформе и операционной системе, на которых работает сервер www, а также уязвимостей в системе управления базами данных веб-сервера и веб-серверах, позволяющие разделить подобные уязвимости на три основные большие группы и создать обобщенные группы уязвимостей, относящихся к этим большим группам, на основе определенных последовательностей. В результате для атаки, осуществляемой на основе каждой уязвимости, можно разработать не единый защитный механизм, а механизм защиты от атак, относящихся к конкретной группе уязвимостей.

Набор уязвимостей веб-сервера состоит из набора уязвимостей всех его компонентов, а именно

$$Z_s = \bigcup_{i=1}^{n} \bigcup_{j=1}^{3} Z_{ij}, \qquad (1)$$

Здесь Z_s – набор уязвимостей всей информационной системы;

Z_{ij} – набор уязвимостей i-го объекта информационной системы j-го уровня группирования;

n – общее количество доступных объектов на веб-сервере;

$m(i,j)$ - общее количество вероятных атак на уязвимости i-го объекта информационной системы j-го уровня группирования.

Набор вероятных реакций веб-сервера на атаку можно получить из следующего выражения:

$$T_{ER} = \bigcup_{i=1}^{n} \bigcup_{j=1}^{3} \bigcup_{k=1}^{m(i,j)} \bigcup_{e=1}^{l(i,j,k)} T_{ijke}, \qquad (2)$$

Здесь T_{ER} – набор вероятностных реакций на атаку;

T_{ijke} - набор реакций на организованную k-ой атаку на уязвимость i-го объекта информационной системы j-го уровня группирования;

n – общее количество доступных объектов на веб-сервере;

$m(i,j)$ - общее количество вероятных атак на уязвимости i-го объекта информационной системы j-го уровня группирования;

$l(i,j,k)$ - общее число вероятностных реакций на атаку, характеризуемых параметрами i, j и k.

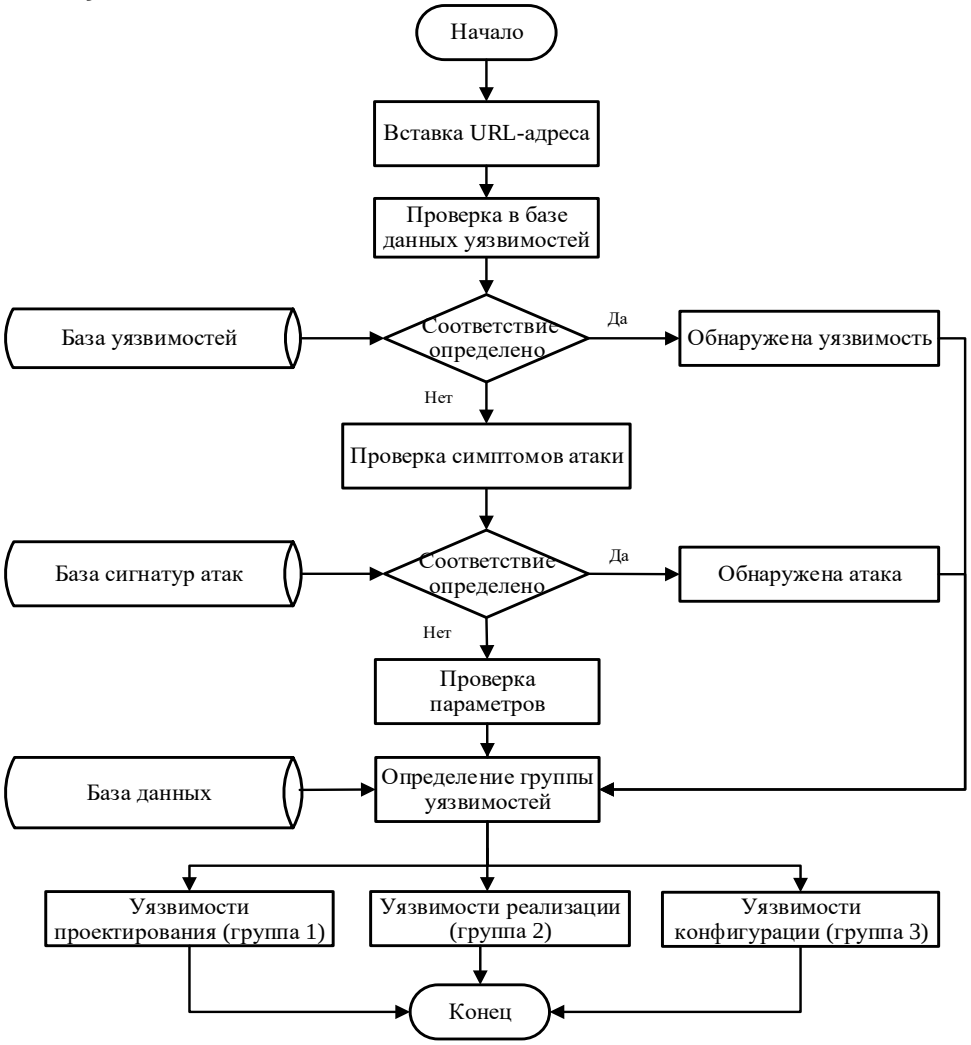


Рисунок 1. Блок-схема алгоритма группирования уязвимостей на веб-сервере

В третьей главе диссертационной работы «**Методы и алгоритмы обнаружения и устранения сетевых атак на веб-серверы**» были разработаны метод и алгоритм обнаружения сетевых атак, нацеленных на третий веб-интерфейс, метод и алгоритм обнаружения сетевых атак VITE, а также модифицированный межсетевой экран устранения сетевых атак.

В первом параграфе сформирован векторный формат данных для описания запроса веб-приложения с учетом статистической структуры запросов и логических категорий веб-страниц. На основе векторного формата разработан метод и алгоритм обнаружения сетевых атак, направленных на веб-интерфейс.

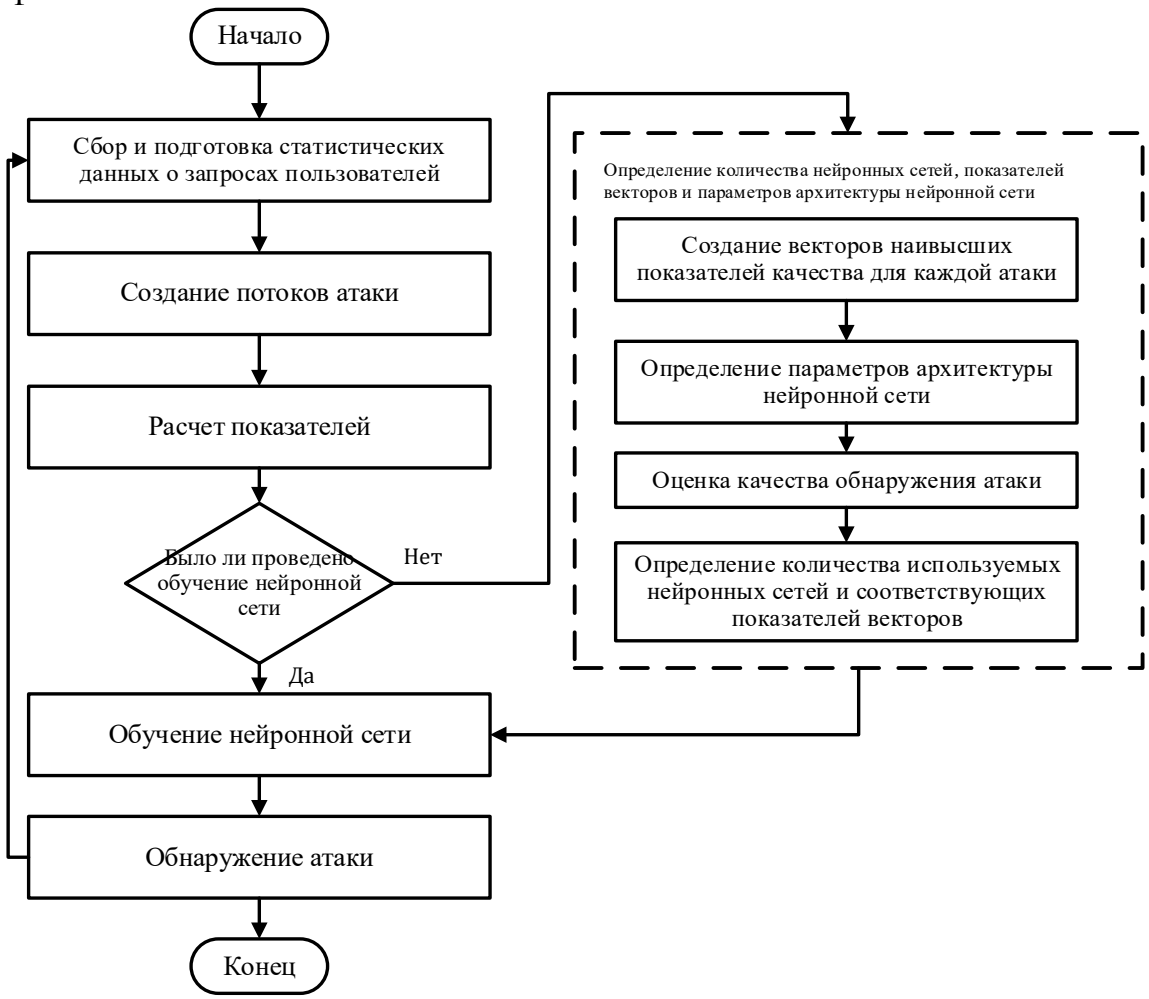


Рисунок 2. Общая схема метода обнаружения атак категории отказа в обслуживании, нацеленных на веб-интерфейс

Суть предлагаемого метода защиты от атак, направленных на веб-интерфейс, заключается в следующем:

1. Подготовка статистической информации о действиях пользователей;
2. Генерация статистической информации о различных категориях последствий атаки, приводящих к отказу в обслуживании;
3. Расчет значений показателей (и соответствующих показателей статистических структур) за рассматриваемый период времени;

4. Формирование наиболее подходящего набора показателей для выявления различных категорий атак, и оценка применения показателей;

5. Определение качества обнаружения атак и наилучших параметров архитектуры нейронных сетей для различных категорий атак;

6. Группирование различных категорий атак по классам атакуемых сил для уменьшения количества используемых нейронных сетей;

7. Обучение нейронных сетей;

8. Использование нейронных сетей для обнаружения атак категории отказа в обслуживании;

9. Переобучение нейронных сетей на основе новой статистики по мере необходимости.

Для описания запроса пользователей к веб-приложениям был разработан следующий векторный формат данных:

($Time_i; SessionID_i; IsSessionStart_i; URL_i; Parameters_i; IP_i; Referer_i; UserAgent_i; Latency_i; DocSize_i; Memory_i; CpuTime_i$);

- $Time_i$– серийный номер запроса в веб-приложениях;
- $SessionID_i$ – идентификатор сеанса;
- $IsSessionStart_i$ – идентификатор начала сеанса;
- URL_i– адрес URL запроса;
- $Parameters_i$- параметры GET-запроса;
- IP_i– IP-адрес, с которому был осуществлен запрос;
- $Referer_i$ – адрес ранее посещенной страницы;
- $UserAgent_i$– строка идентификатора клиентской программы;
- $Latency_i$ – время отклика сервера при обработке запроса;
- $DocSize_i$ – объем информации, загруженной пользователем в ответ на запрос;
- $Memory_i$ - объем оперативной памяти сервера, используемой для обработки запроса;
- $CpuTime_i$– процессорное время ответа на запрос.

Алгоритм обнаружения атак категории отказа в обслуживании, нацеленных на веб-интерфейс, реализован в следующей последовательности.

Первый шаг. Сбор данных о статических и динамических запросах пользователей.

Шаг второй. Передача статической информации о пользовательских запросах в блок потоков атаки.

Шаг третий. Создание потоков атак в системе.

Шаг четвертый. Расчет показателей в потоках атаки. То есть вычисление вероятности того, что это произойдет или не произойдет.

Шаг пятый. Проверка выполнения проверки по нейронной сети.

Шаг шестой. Обучение нейронной сети. При этом, на основе обучения нейронной сети с помощью инструктора выполняются задачи генерации векторов наивысших показателей качества каждой атаки, а также определения параметров сетевой архитектуры и оценки качества обнаружения атаки.

Шаг седьмой. Обнаружение атаки.

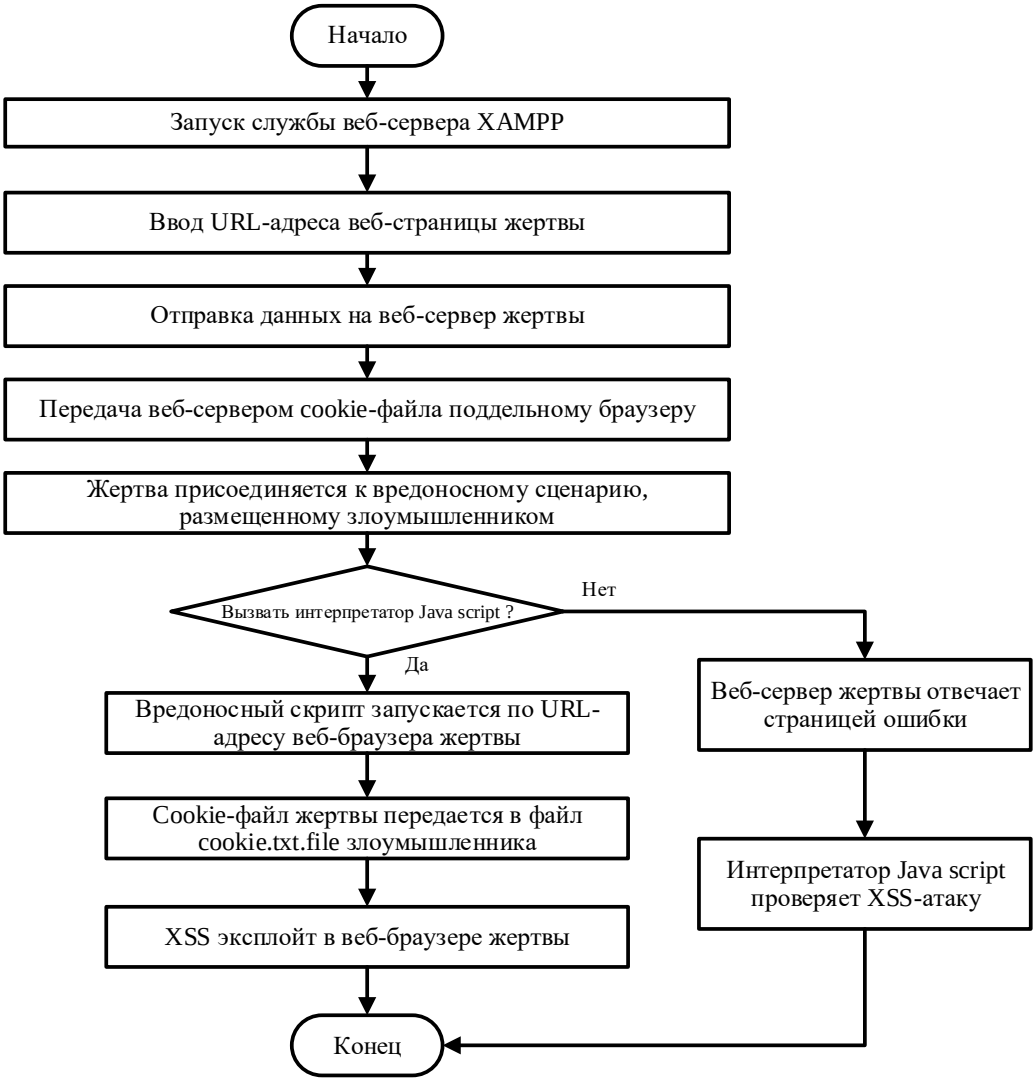


Рисунок 3. Блок-схема алгоритма обнаружения XSS-атаки на сервере LocalHost

Во втором параграфе были разработаны метод и алгоритм VITE для обнаружения сетевых атак в результате создания ограниченной среды, работающей в среде, приводящей сетевые атаки на веб-сервер в безопасное состояние. В результате была обеспечена защита от кражи личных данных пользователя (файлов cookie, идентификаторов сеансов и т.д.) с использованием функций платформ, позволяющих проводить сетевые атаки, нацеленные на веб-сервер.

Количество уголовных дел в киберпространстве растет с каждым годом. Согласно данным топ-10 OWASP, полученным на основании опросов организаций за последние два года, наиболее распространенными атаками являются атаки на основе инъекций, таких как SQL, NoSQL, OS и LDAP. По объявленным данным Whitehat Security, 83 процента заявили, что на сайте имеются как минимум две уязвимости. Для выявления этих уязвимостей нами был предложен метод. Поскольку межсетевой экран, используемый для защиты веб-сайтов должен одновременно контролировать несколько веб-приложений, метод был назван VITE (межсетевой экран веб-приложений).

Метод реализуется в три этапа. Это анализ, выявление и профилактика, то есть устранение. Для этапа анализа целесообразно использовать интеллектуальные методы, которые используются на практике, поскольку эффективность этих методов очень высока, что обосновано и доказано во многих научных работах. Основное внедряемое нововведение было реализовано на этапе выявления и профилактики.

В третьем параграфе предлагается модифицированный межсетевой экран на основе организации современной защиты веб-приложений, работающих на уровне протокола TCP/IP и развернутых в облачных центрах обработки данных, для обнаружения уязвимостей в веб-приложениях, определения новых векторов атак, анализа типов векторов атак SQL-инъекций и защиты веб-приложений от векторов атак OWASP.

Предлагаемый модифицированный режим работы межсетевого экрана и механизм работы реализованы в следующей последовательности. Для этого необходимо выполнить наиболее распространенную атаку SQL-инъекции. Данный метод представляет собой простую SQL-инъекцию на основе ошибок. При этом злоумышленники вводят неожиданные команды, то есть вводят неожиданные команды, т.е. неправильно обращаются к параметрам запроса, например, атаку «человек посередине», перехватывают переменные запроса с помощью каких-либо средств.

Пошаговый алгоритм работы модифицированного межсетевого экрана устранения сетевых атак реализован в следующей последовательности.

Первый шаг. Анализ доступа к деструктивной веб-странице (на стороне клиента) на основе протокола TCP / IP.

Шаг второй. Проверка наличие вредоносного кода на веб-странице URL-адреса или HTML, перехватив HTTP-запроса, который злоумышленник отправил через инструменты на основе обратного прокси-сервера.

Шаг третий. Отправка обнаруженного вредоносного HTTP-запроса на веб-сервер для обработки. Анализ переменных запроса HTTPS, а также выявление уязвимостей в переменных запроса аналитика.

Шаг четвертый. Перенос запроса на веб-сервер без вектора атаки в противном случае отправка запроса в модуль защиты для классификации вредоносных кодов.

Шаг пятый. Классификация чтобы проверить, связан ли вектор атаки с SQL-инъекцией или другим OWASP. Если OWASP имеет отношение к определение категорий входных переменных.

Шаг шестой. Блок IP, управление журналом и отправка сообщения защиты от атаки SQL-инъекции с предупреждением владельцу сервера об атаке.

Шаг седьмой. Анализ отправленных злоумышленником сообщений об ошибках, проверка обхода авторизации на уровне приложения и базы данных.

Шаг восьмой. Обработка запроса веб-сервером и возврат персонализированного сообщения об ошибке в качестве ответа.

Шаг девятый. Завершение.

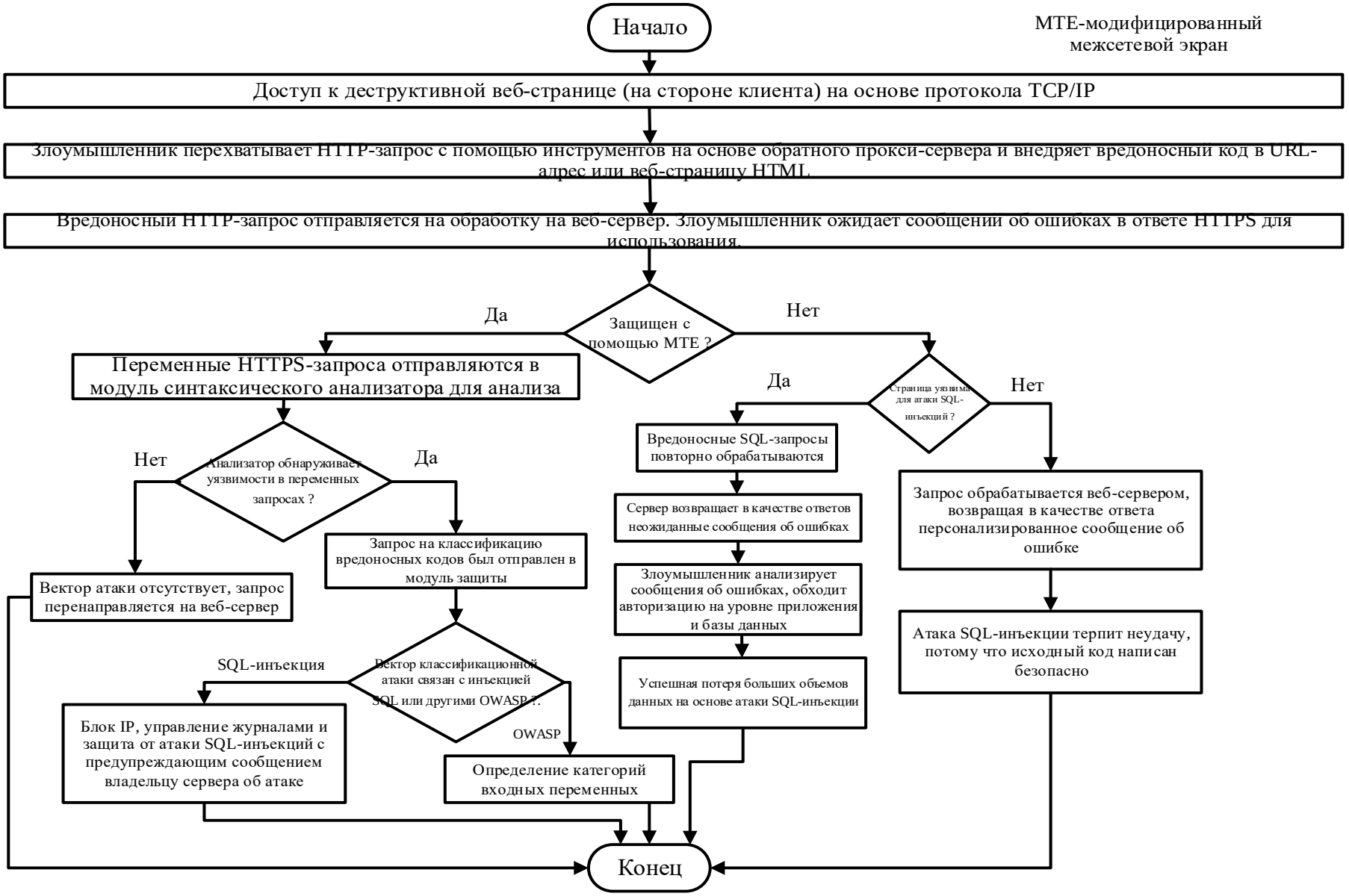


Рисунок 4. Схема работы модифицированного межсетевого экрана устранения сетевых атак

В четвертой главе диссертации **«Оценка эффективности процесса обнаружения сетевых атак и результаты их применения на практике»** представлена оценка эффективности методов обнаружения уязвимостей и сетевых атак, функциональная структура и принцип работы программного средства обнаружения сетевых атак, а также результаты экспериментов-расчетов, полученных в результате внедрения.

В первом параграфе проведена оценка эффективности методов обнаружения уязвимостей и сетевых атак.

Центром кибербезопасности был дан ряд рекомендаций по выявлению уязвимостей и сетевых атак, а также повышению эффективности обеспечения информационной безопасности. Такие как:

1. Использование лицензионных и сертифицированных операционных систем и программ.

2. Регулярное обновление до последней версии существующих операционных систем, программного обеспечения и компонентов безопасности. Проведение работ по обновлению из официальных источников.

3. Использование плагинов безопасности с функциями поиска, удаления и защиты от вредоносных программ в будущем.

4. Регулярно выполнять резервное копирование баз данных, файлов, почты и т.п.

5. Удаление неиспользуемых плагинов.

6. Усиление аутентификации на основе пароля.

7. Обеспечить доступ к информационной системе или веб сайту с устройств (компьютеров, планшетов) на которых установлены антивирусные программы с обновленными вирусными базами.

8. Проведение экспертиз информационных систем и ресурсов на соответствие требованиям информационной безопасности. Своевременное устранение выявленных уязвимостей на основании рекомендаций, направленных по результатам экспертизы.

9. Систематическое повышение уровня квалификации и знаний пользователей (сотрудников) в области информационно-коммуникационных технологий и информационной безопасности.

10. Быстрое обнаружение и принятие соответствующих мер для устранения угроз и последствий инцидентов кибербезопасности.

Таблица 1

Результаты тестирования метода трехэтапного тестирования для обнаружения уязвимостей на серверах.
инъекционные уязвимости (ИУ), уязвимость бизнес- логики(УБЛ), уязвимость фиксации сеансов(УФС)

Типы уязвимостей	Общее количество уязвимостей	выявленных уязвимостей	невыявленных уязвимостей	ложных срабатываний системы
ИУ	23	22	0	1
УБЛ	11	10	1	0
УФС	16	15	1	0

Таблица 2

Результаты оценки эффективности метода трехэтапного тестирования для обнаружения уязвимостей на веб-серверах

Здесь программа обнаружения уязвимостей на веб-сервере (ПОУВС).

Программа обнаружения уязвимостей	Всего уязвимостей	выявленных уязвимостей	невыявленных уязвимостей	ложных срабатываний системы
ПОУВС	26	25	1	0
Acunetix	26	24	2	0
H-X Scanner	26	23	2	1
ImmuniWeb	26	22	3	1
Quttera	26	24	0	2

Рисунок 5. Результаты оценки эффективности метода трехэтапного тестирования для обнаружения уязвимостей на веб-серверах

Во втором параграфе представлена функциональная структура программного средства обнаружения сетевых атак (рис. 6).

Программное средство работает как прокси-сервер, но также выполняет дополнительные функции - возможность исследовать HTTPS-трафик путем проверки определенного сертификата сервера. Это функции:

- балансировка и контроль объема запросов на веб-сервере;
- остановка трафика SSL и другие подобные функции.

Разработанное программное средство осуществляет подключение к веб-серверу следующим образом:

- в режиме мониторинга сети в реальном времени с портом SPAN;
- режим прокси: прозрачный, мост и обратный режим.

В третьем параграфе представлены результаты внедрения в практику программного средства обнаружения уязвимостей веб-сервера организации.

Программное средство для обнаружения открытых портов на веб-сервере и уязвимостей в них, а также защиты данных на веб-сервере от сетевых атак внедрено в ГУП «Центр кибербезопасности», ООО «UZINFOCOM Единый

интегратор по созданию и поддержке государственных информационных систем» и ООО «MAXSUS XIZMAT BUX», результаты приведены ниже.

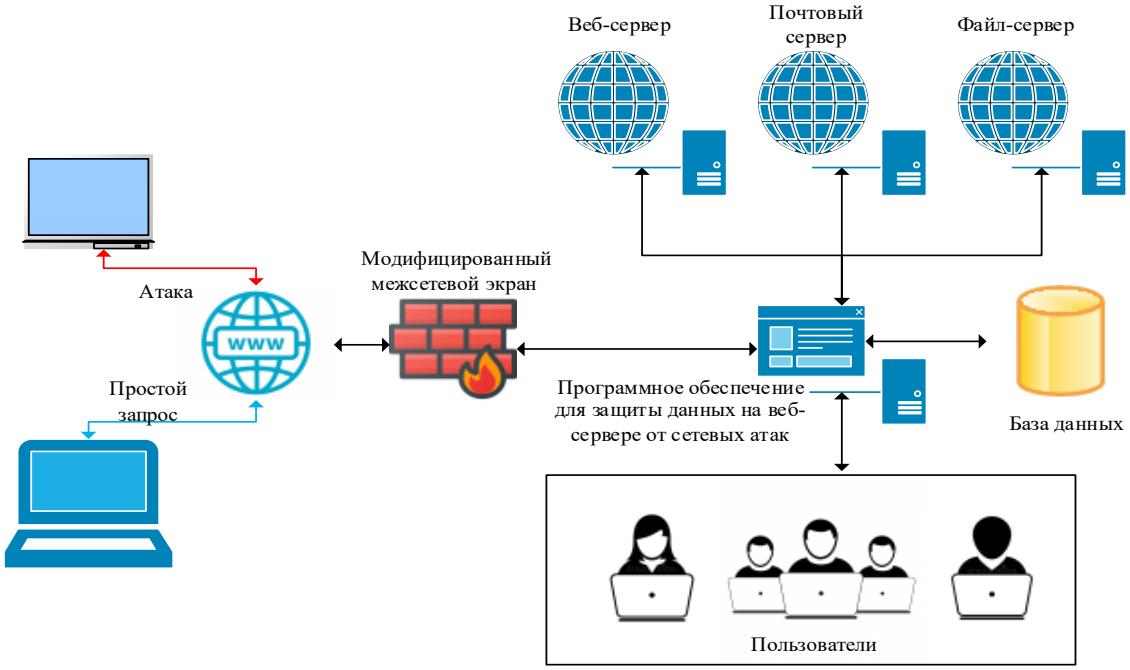


Рисунок 6. Функциональная структура программного средства защиты данных на веб-сервере от сетевых атак

Разработанное программное средство для обнаружения открытых портов на веб-сервере и уязвимостей в них, а также для защиты данных на веб-сервере от сетевых атак позволило обнаружить 152348 сетевых атак с точностью 98,7% и регистрацией ошибок 1,3% в ГУП «Центр кибербезопасности». В ходе тестирования было подтверждено, что функция оповещения системного администратора об ошибках работает в режиме реального времени.

В ООО «UZINFOCOM Единый интегратор по созданию и поддержке государственных информационных систем» проведены экспериментальные испытания с целью выявления открытых портов на веб-сервере и уязвимостей в них, а также защиты данных на веб-сервере от сетевых атак. Разработанное программное средство в результате тестирования позволило обнаружить 153 открытых порта и 6 типов уязвимостей на веб-сервере, а также 163469 сетевых атак с точностью 97,9% и регистрацией ошибок 2,1%. Исходя из полученных результатов, можно сказать, что использование этого программного средства позволило одновременно обнаружить открытые порты и уязвимости на веб-сервере, а также сетевые атаки.

В ООО «MAXSUS XIZMAT BUX» было проведено тестирование с целью выявления открытых портов на веб-сервере и уязвимостей в них, а также защиты данных на веб-сервере от сетевых атак. Разработанное программное средство в результате тестирования позволило обнаружить 148 открытых портов и 6 типов уязвимостей на веб-сервере, а также 135238 сетевых атак с точностью 97,5% и регистрацией ошибок 2,5%. Результаты тестирования показали, что использование данного программного средства позволило одновременно эффективно обнаружить открытые порты и уязвимости на веб-сервере, а также сетевые атаки.

ЗАКЛЮЧЕНИЕ

В результате исследований по диссертационной работе на тему «Методы и алгоритмы защиты информации на веб-серверах от сетевых атак» были представлены следующие выводы:

1 На основе статистических данных, сформированных, организацией US-CERT Open Information Security Foundation, был сформирован реестр уязвимостей на веб-серверах, который группирует уязвимости разработчиков программного продукта в своих приложениях в единую систему идентификации (например, CVE-ID). Результат позволил интегрировать уязвимости веб-сервера и типы атак, на которых они основаны, в базу данных уязвимостей OWASP.

2 В результате тестирования веб-приложений, состоящих из трех классов, был разработан метод трехэтапного тестирования и алгоритм обнаружения уязвимостей на веб-серверах. Результатом стал полный доступ к различным типам наборов данных для обнаружения уязвимостей на веб-серверах и приложениях.

3 Разработан метод и алгоритм группирования уязвимостей на веб-серверах, позволяющий создавать обобщенные группы. В результате получен не защитный механизм для атаки, осуществляемой на основе каждой уязвимости, а возможность разработки защитного механизма для атак, относящихся к группе уязвимостей.

4 Векторный формат данных был сформулирован для описания запроса веб-приложений с учетом статистической структуры запросов и логических категорий веб-страниц. На основе векторного формата разработаны метод и алгоритм обнаружения сетевых атак, направленных на веб-интерфейс. В результате это позволило защитить запросы атаки, направленные на веб-интерфейс, от несанкционированного доступа к базе данных.

5 В результате создания ограниченной среды были разработаны метод и алгоритм VITE для обнаружения сетевых атак. В результате появилась возможность защиты от кражи личных данных пользователя (cookie файлов, идентификаторов сеансов и т.д.) с помощью функций платформ, позволяющих проводить сетевые атаки, нацеленные на веб-сервер.

6 Программное средство защиты данных на веб-сервере от сетевых атак, разработанное на основе метода трехэтапного тестирования обнаружения уязвимостей и методов VITE обнаружения сетевых атак, позволил обнаружить уязвимости с точностью 96,1% а атаки - с точностью 97,9%. Были даны рекомендации по достижению лучшего показателя эффективности при выявлении уязвимостей.

Разработанное на основе предложенных методов программное средство защиты данных на веб-сервере от сетевых атак позволяет повысить эффективность систем информационной безопасности, используемых для защиты веб-серверов и приложений на предприятиях и в организациях, а также сохранить удобство использования веб-приложений.

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

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

IBROKHIMOV AZIZBEK RAVSHANBEK UGLI

METHODS AND ALGORITHMS FOR PROTECTING INFORMATION ON WEB SERVERS FROM NETWORK ATTACKS

05.01.05 – Methods and systems of information protection. Information security

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON TECHNICAL SCIENCES

Tashkent-2024

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Ministry of Higer Education, Science and Innovations of the Republic of Uzbekistan under number B2023.3.PhD/T4056.

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:	**Khamdamov Rustam Khamdamovich** doctor of Technical Sciences, professor
Official opponents	**Jurayev Gayrat Umarovich** doctor of Physical and Mathematical sciences, associate professor
	Nasrullayev Nurbek Bakhtiyorovich doctor of philosophy in technical sciences, associate professor
Leading organization:	**Scientific-Engineering and Marketing researches center "UNICON.UZ" LLC**

The defense will take place "24" January 2024 at 11:30 the meeting of Scientific council No. DSc 13/30.12.2019.T.07.02 at Tashkent University of Information Technologies (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No.187. (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43).

Abstract of dissertation sent out on "12" January 2024 y.
(mailing report No. 4 on "11" January 2024 y.)

B.Sh. Makhkamov
Chairman of the scientific council awarding scientific degrees, doctor of economical sciences, professor

M.S. Saitkamolov
Scientific secretary of scientific council awarding scientific degrees, doctor of economical sciences, associate professor

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

INTRODUCTION (abstract of PhD thesis)

The aim of the research work is to develop methods and algorithms for protecting information from network attacks, which allow to increase the efficiency of the web server protection system.

The object of the research work is the process of identifying vulnerabilities in the web server and protecting information from network attacks.

The scientific novelty of the research work is as follows:

on the basis of statistical data collected by international organizations, a registry of vulnerabilities on web servers was created, which groups vulnerabilities in a single identifier system;

as a result of testing web applications consisting of three classes, a three-step testing method for detecting vulnerabilities in web servers has been developed;

developed a method and algorithm for grouping vulnerabilities in web servers, which allows creating generalized groups based on communication channel, protocol, and hardware platform groups on which the web server operates;

a method and algorithm for detecting network attacks aimed at the web interface was developed based on the vector format formed taking into account the statistical structure of requests and the logical categories of web pages;

The VITE method and algorithm for detecting network attacks have been developed as a result of creating a limited environment that works in an environment that makes network attacks on the web server safe.

Implementation of the research results. Based on the scientific results obtained on the methods and algorithms and software tools to protect the information on the web server from network attacks:

The software tool developed on the basis of methods and algorithms for protecting information on the web server from network attacks has been implemented in the practical activity of the state unitary enterprise “Cybersecurity Center” (Information No. 33-8/6723 dated October 11, 2022 of the Ministry of Information Technologies and Communications Development). The result of the scientific research made it possible to identify 152,348 network attacks in the corporate network with 98.7% accuracy and 1.3% error;

The software tool, developed on the basis of methods and algorithms for protecting information on the web server from network attacks, was introduced into the practical activities of the limited liability company “UZINFOCOM Single Integrator for the Creation and Support of State Information Systems” (2022 of the Ministry of Information Technologies and Communications Development Reference No. 33-8/6723 dated October 11). As a result of scientific research, it was possible to identify 153 open ports and 6 types of vulnerabilities in the organization's web server, as well as 163,469 network attacks with 97.9% accuracy and 2.1% error;

The software tool, developed on the basis of methods and algorithms for protecting information on the web server from network attacks, was introduced into the practical activities of the limited liability company “MAXSUS XIZMAT BUX” (Information No. 33-8/6723 dated October 11, 2022 of the Ministry of Information Technologies and Communications). The result of the scientific research allowed to

identify 148 open ports and 6 types of vulnerabilities in the organization's web server and 135238 network attacks with 97.5% accuracy and 2.5% error.

Structure and volume of the dissertation. The dissertation consists of an introduction, four chapters, a conclusion, a list of references and appendices. The volume of the dissertation is 115 pages.

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

I bo‘lim (I часть; I part)

1. R.Khamdamov, A.Ibrokhimov. Techniques and methods of BLACK BOX identifying vulnerabilities in web servers // International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities (ICISCT 2021). Tashkent-2021. -4p. (3) Scopus (ОАК раёсатининг қарори 30.09.2021 йил №525)
2. R.Khamdamov, A.Ibrokhimov. Web application firewall method for detecting network attacks // International Conference on “Information Science and Communications Technologies: Applications, Trends and Opportunities (ICISCT 2021). Tashkent-2021. -3p. (3) Scopus (ОАК раёсатининг қарори 30.09.2021 йил №525)
3. A.Ibrokhimov. Detection method for “Denial os service” attacks on web applications // Chemical technology. Control and management, Tashkent-2020, №3(93), p. 59-65. (05.00.00; №12)
4. Р.Хамдамов, А.Иброхимов, Веб серверлардаги заифликларни аниқлашнинг модификацияланган қора қути усули ва алгоритмлари // “Илмий хабарнома Физика –математика тадқиқотлари” журнали. 2021/№2(20). Андижон-2021. –Б. 15-21. (13.00.00; №12)
5. А.Иброхимов, Веб серверлардаги заифликларни гуруҳлаш усули ва алгоритми // “Муҳаммад ал-Хоразмий авлодлари” журнали. № 3(21), Тошкент-2022. –Б. 187-191. (05.00.00; №10)
6. Botirov F.B., Ibrohimov A.R., Veb interfeysga qaratilgan tarmoq hujumlarini aniqlash usuli va algoritmi // “Spectrum Journal of Innovation, Reforms and Development”. ISSN (E): 2751-1731. VOLUME 20, October, USA-2023. –P. 55-60 (№23)

II bo‘lim (II часть; II part)

7. Ibrohimov A.R., Корпоратив тармоқларнинг веб серверларига бўладиган ҳужумлар ва улардан ҳимояланиш тенденциялари // International Conference “ICT In education: challenges and solutions” Tashkent-2021 – Б . 81-83.
8. Xamdamov R.X., Ibrohimov A.R., Korporativ tarmoq muammolarini yechish yo‘llari // “Axborot kommunikatsiya texnologiyalari va dasturiy ta’minot yaratishda innovatsion g‘oyalar” Respublika miqyosidagi ilmiy-texnik anjumani materiallari to‘plami. I-tom. Samarqand-2021. –B. 195-198.
9. Khamdamov R.Kh, A.Ibrokhimov, Network firewall with modifications to eliminate attacks // Сборник докладов республиканской научно-технической конференции «Современное состояние и перспективы развития

цифровых технологий и искусственного интеллекта». Часть 1. Ташкент-2022. -P. 261-265.

10. A.Ibrokhimov. The Structure of the Vulnerability Detection System on Web Servers // 2nd International Conference on Pervasive Computing and Social Networking (ICPCSN 2022). Salem, India March-2022. -7p. (3) Scopus

11. Xamdamov R.X., Haydarov E.D, Ibrohimov A.R, Logistik regressiya asosida tasniflash masalalarini yechish // Multidisciplinary Scientific Journal “RESEARCH AND EDUCATION”. ISSN: 2181-3191. VOLUME 1, ISSUE 9, December, USA-2022. –B. 162-171

12. Ibrohimov A.R, Haydarov E.D., Evalution of the effectiveness of methods of detecting weaknesses and network attacks // “Spectrum Journal of Innovation, Reforms and Development”. ISSN (E): 2751-1731. VOLUME 20, October, USA-2023. –P. 55-60

13. Ibrohimov A.R, Haydarov E.D., Vite method and algorithm of network attack detection // ACADEMIC INTERNATIONAL CONFERENCE ON “MULTI-DISCIPLINARY STUDIES AND EDUCATION”. Hosted from Pittsburg, USA-2023. –P. 117-120.

14. Ibrohimov A.R, Haydarov E.D., Tarmoq hujumlarini aniqlashni dasturiy vositasining funksional strukturasi // “SCIENCE PROMOTION”. Vol. 2, Farg‘ona-2023. –B. 115-118

15. Ibrohimov A.R, Haydarov E.D., Web serverlardagi tarmoq hujumlarini aniqlashni dasturiy vositasi // “SCIENCE PROMOTION”. Vol. 2, Farg‘ona-2023. –B. 119-121

16. R.X.Xamdamov, A.R.Ibrohimov, Veb serverdagi ma’lumotlarni tarmoq hujumlaridan himoyalash dasturi // Dasturga guvohnoma № DGU 13394. Toshkent 04.12.2021.

17. R.X.Xamdamov, A.R.Ibrohimov, Veb serverdagi zaifliklarni aniqlash dasturi // Dasturga guvohnoma № DGU 13395. Toshkent 04.12.2021.

18. R.X.Xamdamov, A.R.Ibrohimov, Veb serverdagi ochiq portlar va ulardagi zaifliklarni aniqlash dasturi // Dasturga guvohnoma № DGU 13396. Toshkent 04.12.2021.

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

Bosishga ruxsat etildi: 12.12.2023-yil
Bichimi: 60x84 $^{1}/_{16}$. “Times New Roman” garniturada
raqamli bosma usulda bosildi.
Nashriyot bosma tabog‘i: 2.5. Adadi: 100 dona. Buyurtma № 50
Bahosi kelishuv asosida

Nizomiy nomidagi Toshkent davlat pedagogika
Universiteti bosmaxonasida chop etildi.
Manzil: Toshkent shahar, Chilonzor tumani,
Bunyodkor ko‘chasi 27-uy.