ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕСИТЕТИ

Қўлёзма ҳуқуқида
УДК 004.056.57

Рахматов Дилшод Нигматиллаевич

ОЧИҚ КОДЛИ ОПЕРАЦИОН ТИЗИМЛАРГА ЗИЁН КЕЛТИРУВЧИ ДАСТУРЛАРДАН ҲИМОЯЛАШНИНГ ДАСТУРИЙ ВОСИТАЛАРИ

05.13.19 – Ахборотларни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги

техника фанлари номзоди илмий даражасини олиш учун тақдим этилган диссертация

А В Т О Р Е Ф Е Р А Т И

Тошкент – 2011

Иш Ўзбекистон алоқа ва ахборотлаштириш агентлиги ва Тошкент ахборот технологиялари университетида бажарилган

Илмий раҳбар	техника фанлари доктори, профессор **Қосимов Содиқжон Собирович**
Расмий оппонентлар:	техника фанлари доктори, академик **Бекмуратов Тўлқин Файзиевич**
	техника фанлари номзоди, доцент **Ахмедова Ойдин Пулатовна**
Етакчи ташкилот	Ўзбекистон Миллий университети

Ҳимоя Тошкент ахборот технологиялари университети хузуридаги Д 001.25.01 рақамли ихтисослашган кенгашнинг 2011 йил "24" ноябрь соат 9⁰⁰ да ўтадиган мажлисида бўлади. Манзил: 100084, Тошкент ш., Амир Темур кўчаси, 108, e-mail: d.ganievaa@rambler.ru.

Диссертация билан Тошкент ахборот технологиялари университети кутубхонасида танишиш мумкин.

Автореферат 2011 йил "18" октябрь да тарқатилди.

Ихтисослашган кенгаш
илмий котиби А.А.Ганиев

ДИССЕРТАЦИЯНИНГ УМУМИЙ ТАВСИФИ

Мавзунинг долзарблиги. Бугунги кунда очиқ кодли операцион тизимлар (ОКОТ) жадал суръатларда ривожланиб бормоқда. ОКОТ га мисол тариқасида UNIX оиласига мансуб Linux тизимларини келтириш мумкин. Дунёда Linux операцион тизимининг (ОТ) мингдан ортиқ турлари мавжуд бўлиб, улар Linux ОТ дистрибутивлари деб аталади. Дистрибутив бу – алоҳида гуруҳ ёки компания томонидан бир мақсад учун яратилган дастурлар тўпламидир. Дистрибутив Linux операцион тизимининг тўлиқ версиясини ўрнатиш учун барча зарур компонентларга эга. Шу билан бирга, дистрибутивлар компонентлар тўплами билан бир-биридан фарқ қилиши мумкин, уларнинг ҳар бири турли жиҳатларга эга. Масалан, бир дистрибутив ундан фойдаланиш ва уни ўрнатишнинг қулайлиги билан ажралиб турса, бошқа дистрибутив фойдаланувчини турли хил кўплаб иловалар билан таъминлай олади. Бугунги кунда ОКОТларга хос асосий хусусият - хавфсизлик, барқарорлик ва тезкорлик. Юқоридаги сифатларни инобатга олган ҳолда, кўплаб фирмалар, компаниялар ва давлат корхоналари сервер сифатида ОКОТдан фойдаланади. Айни пайтда, ОКОТдан фойдаланиш доирасининг кенгайиши уларга зиён келтирадиган дастурлар каби янги таҳдидларнинг пайдо бўлишига олиб келди. Бундай дастурлар ҳимояланмаган ОКОТ серверларини ишдан чиқариши, уларнинг ишлаш самарадорлигини сезиларли даражада пасайтириши ва маълумотларнинг йўқолишига олиб келиши мумкин. Зиён келтирувчи дастурлар ахборот муҳитининг хавфсизлигига хавф солувчи энг жиддий таҳдидларнинг алоҳида тоифасига киради. Шу сабабли бундай хилдаги хавфларни аниқлаш ва бартараф қилиш ОКОТ учун ҳам долзарб муаммо ҳисобланади.

Муаммонинг ўрганилганлик даражаси. Ахборот хавфсизлигини таъминлаш йўналишида тадқиқот олиб бораётган К.Лендвер, Д.МакЛин, М.Гук, Р.Сандху, К.Брайс, В.Герасименко, С.П.Расторгуев, А.Ю.Шчербаков, Л.М.Ухлинов, Е.Касперский, И.С.Пахамов, М.Н.Арипов, Д.А.Абдуллаев, Т.Ф.Бекмуратов, С.С.Касимов, М.М.Каримова, С.К.Ганиев, З.Т.Адилова, П.Ф.Хасанов, Р.Х.Хамдамов ишлари билан яқиндан танишиб чиқилди.

Шу билан бирга, кўпчилик муаллифларнинг тадқиқотлари шуни кўрсатиб турибдики, зиён келтирувчи дастурларни аниқлаш ва блокировкалашнинг мавжуд усуллари фойдаланишда ва ахборот хавфсизлигини оширишда чегараланган бўлиб, бу усуллар ОКОТ ишлаш тезлигининг маълум даражада пасайишига ҳам олиб келмоқда. Ахборотнинг тобора кўпайиб бориши ҳамда уни қайта ишлаш усулларининг мураккаблашиб бориши, шунингдек янги кўринишдаги хавф-хатарлар ва зиён келтирувчи дастурларнинг пайдо бўлиши, ОКОТларга хавфларни ўз вақтида аниқлаш ва уларни олдини олиш вазифаларини қўймоқда. Бугун бундай вазифалар анъанавий алгоритм усулларидан фақат биттасидан фойдаланиш ва битта мезонни ҳисобга олиш орқали ҳал қилинмоқда.

Ахборот хавфсизлиги тизимининг самарадорлигини ошириш муаммоларини ҳал қилиш ҳимоя усуллари ва кўрсаткичларидан, шу жумладан, экспертлар билимлари, продукцион моделлар ва мантикий мулоҳазаларга асосланган эвристик усуллардан фойдаланишни тақозо этади.

Диссертация ишининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация иши Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Фан ва технологияларни ривожлантиришни мувофиқлаштириш қўмитасининг №17-003 сонли "Миллий эркин ва очиқ кодли дастурий таъминотни яратиш" (2009-2011й.) илмий-тадқиқот иши доирасида бажарилган.

Тадқиқот мақсади. Зиён келтирувчи дастурларни аниқлаш ва олдини олиш учун алгоритм ва дастурий воситаларни очиқ кодли операцион тизим ядроси даражасида ишлаб чиқиш.

Тадқиқот вазифалари. Диссертация ишида қўйилган мақсадга эришиш учун қуйидаги вазифалар ҳал этилади:

1. Очиқ кодли операцион тизимларда зиён келтирувчи дастурларга қарши курашиш хусусиятларини аниқлаш ва таҳлил қилиш.
2. Қайта ишлашнинг статистик ва эвристик усуллари билан бирга изоляция қилиш принципига асосланган очиқ кодли операцион тизимларга зиён келтирувчи дастурларни изоляция қилишнинг мукаммал усулини ишлаб чиқиш.
3. Зиён келтирувчи дастурларнинг ҳаракатлари хусусиятлари таҳлилидан фойдаланган ҳолда, ОКОТларни ҳимоялаш алгоритмларини ишлаб чиқиш.
4. Зиён келтирувчи дастурларни изоляция қилиш ва блокировкалашнинг эксперт тизимлари асосида ОКОТнинг ҳимоя тизимини яратиш.
5. ОКОТ ядроси даражасида, зиён келтирувчи дастурлардан ҳимоялашнинг дастурий воситаларини яратиш.
6. Зиён келтирувчи дастурлардан ОКОТни ҳимоя қилишнинг дастурий воситаларини эксперементал синовдан ўтказиш ва улардан фойдаланишга доир тавсиялар ишлаб чиқиш.

Тадқиқот объекти ва предмети. Очиқ кодли операцион тизимларни зиён келтирувчи дастурлардан ҳимоя қилишнинг алгоритмлари ва дастурий воситалари тадқиқот объекти ҳисобланади.

«Linux» тоифасидаги очиқ кодли операцион тизимларнинг ахборот хавфсизлиги тадқиқот предмети ҳисобланади.

Тадқиқот методлари. Тадқиқот ишида ахборот ҳимоясига хавф солувчи таҳдидларни аниқлаш усуллари, ихтиро масалаларини ечиш назарияси, эксперт тизим продукцион усуллари, алгоритмлар назарияси ва объектга мўлжалланган дастурлашлардан фойдаланилган.

Тадқиқот гипотезаси. ОКОТларга, зиён келтирувчи дастурларни блокировкалашни янада мукаммаллаштириш ва зиён кўрилганда уларнинг ишлаш қобилиятини тиклашда, кашф қилиш масалалари назарияси ва

комплексли алгоритмик ва эвристик процедураларни қайта ишлаш асосида изоляция қилишдан фойдаланиш, муаммоларни олдини олиш имкониятини беради.

Ҳимояга олиб чиқилаётган асосий ҳолатлар:

1. Турли алгоритм ва эвристик усуллар ва технологияларни изоляция қилиш ва улардан комплекс фойдаланиш принципларига асосланган ОКОТ ҳимояси концепцияси.

2. Зиён келтирувчи дастурларни изоляциялаш ва блокировкалаш принципларига асосланган ОКОТни ҳимоя қилиш усуллари ва алгоритмлари.

3. ОКОТга зиён келтирувчи дастурларни изоляция ва блокировкалашнинг эксперт тизими.

4. Зиён келтирувчи дастурларни изоляция қилиш жараёнларини моделлаштириш алгоритми.

5. ОКОТни зиён келтирувчи дастурлардан ҳимоя қилувчи дастурий воситалар.

Илмий янгилиги. Диссертациядан олинган натижаларнинг илмий янгилиги қуйидагилардан иборат:

1. ОКОТ ҳимояси концепциясига асосланган зиён келтирувчи дастурларни блокировкалашнинг модификацияланган усули ва алгоритми таклиф этилди.

2. Зиён келтирувчи дастурлардан ОКОТ ядросини ҳимоя қилиш воситалари тўғрисидаги билимларнинг продукцион модели яратилди.

3. Иловалар даражасида зиён келтирувчи дастурларни изоляция қилишнинг моделлаштириш алгоритми ишлаб чиқилди.

4. Зиён келтирувчи дастурларни блокировкалаш ва изоляция қилишнинг эксперт тизими тузилмаси яратилди, унинг доирасида ҳимоя воситалари танлови бўйича реал вақтда қарорлар қабул қилиш методикаси таклиф этилди.

5. ОКОТ ҳимоя тизимларига зиён келтирувчи дастурлар таъсирини блокировкалаш ва изоляция қилиш дастурлари ишлаб чиқилди.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқотнинг илмий аҳамияти, ОКОТ ҳимояси усулларини тизимлаштириш ҳамда шулар асосида зиён келтирувчи дастурларни изоляциялаш ва блокировкалаш усуллари ва моделларини модификациялашни ишлаб чиқишдан иборат. Тавсия этилаётган усул ва моделлар ҳар хил ахборот тизимларида зиён келтирувчи дастурлардан ҳимояловчи мукаммал алгоритм ва дастурларни яратиш имкониятини беради.

Натижанинг амалий аҳамияти эса яратилган моделлар, алгоритмлар ва дастурий воситалар реал вақт ичида хавфни баҳолаш ва ҳимоялаш воситасини танлашга қарор қилувчи эксперт тизимларини яратади.

Натижаларнинг жорий қилиниши. Диссертация ишининг назарий ва амалий натижалари очиқ кодли операцион тизимларнинг ишлаш самарадорлигини ошириш ва уларда ахборот ҳимоясини таъминлаш

масалаларини ечиш учун алгоритмлар «DosTlink» Интернет провайдерида амалга оширилди.

Тадқиқот натижалари бўйича эркин ва очиқ дастурий таъминотларни ривожлантириш, шунингдек Ўзбекистон Республикасининг 200та туманидаги касб-ҳунар коллежлари ва академик лицейларда UzMOT 1.0 операцион тизимини тарқатиш бўйича «Келажак овози - 2010», «Ўзбекистон маданияти ва санъати форуми» (Фонд Форум) ёзги ўқув лагерида тренинглар ўтказилди.

Тадқиқот натижалари ўқув дастурларига киритилади ва Тошкент ахборот технологиялари университети ўқув жараёнида "Электрон тижорат тизимлари хавфсизлиги", "Linux операцион тизими асослари" фанлари бўйича маъруза, амалий ва лаборатория машғулотларини ўтказишда ҳамда 5А523509 – "Ахборот хавфсизлиги" ва 5А523601 – "Электрон тижорат" мутахассисликлари бўйича магистрлик диссертациясини бажаришда фойдаланилади.

Ишнинг синовдан ўтиши. Диссертация ишининг асосий мавзулари «Ал-Хоразмий 2009 – амалий математика ва ахборот технологияларининг долзарб муаммолари» халқаро илмий анжуманида (Тошкент, 2009 йил), «Ахборот-коммуникация технологияларини ривожлантириш муаммолари ва кадрлар тайёрлаш» халқаро илмий анжуманида (Тошкент, 2009 йил), «Ахборотлаштириш соҳасида ахборот хавфсизлиги. Муаммолар ва уларни ҳал қилиш» Республика семинарида (Тошкент, 2009 йил), AICT2010 ахборот-коммуникация технологияларидан фойдаланиш бўйича IEEE тўртинчи халқаро анжуманида (Тошкент, 2010 йил) муҳокама этилди ва улар бўйича маърузалар тингланди.

Натижаларнинг эълон қилинганлиги. Тадқиқотнинг асосий натижалари 10та журнал мақолаларида чоп этилди, «UzMOT 1.0 операцион тизими» (№DGU 01899) ва «Uz-Booyo 1.0 операцион тизими» (№DGU 01547) ЭҲМ учун дастурларни расмий рўйхатдан ўтказиш тўғрисида гувоҳномалар олинди.

Диссертациянинг тузилиши ва ҳажми. Диссертация иши кириш, тўртта бўлим, хулоса, илова ва адабиётлар рўйхатидан иборат. Тадқиқот машинада чоп этилган 133 варақда (шу жумладан 19 та расмда, 7 та жадвалда ва 102 номдаги адабиётлар рўйхатида) баён этилган.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация иши мавзусининг долзарблиги, муаммонинг ўрганилганлик даражаси, тадқиқот объекти ва предмети, шунингдек, тадқиқотнинг мақсади ва вазифалари аниқланиб асослаб берилди. Илмий ишни бажаришда фойдаланилган тадқиқот методлари, тадқиқотнинг илмий янгилиги, тадқиқот натижаларининг илмий ва амалий аҳамияти, ҳимояга олиб чиқилаётган асосий ҳолатлар, тадқиқотнинг

апробациядан ўтганлиги, натижаларнинг эълон қилинганлиги, диссертация ишининг тузилиши ва ҳажми тўғрисидаги ахборотлар баён этилган.

Диссертация ишининг биринчи бўлимида очиқ кодли операцион тизимларга зиён келтирувчи дастурлар турлари ва хавфлари, зиён келтирувчи дастурлар таъсирини изоляция қилиш усуллари ва уларга ыарши курашиш хусусиятлари ёритиб берилган.

ОКОТга таъсир қилувчи зиён келтирувчи дастурларни таҳлил қилиш тарқалиш усули ва уларни амалга ошириш алгоритмлари турлари бўйича уларни таснифлаш мумкинлигини кўрсатмокда. Зиён келтирувчи дастурларнинг тарқалиш усулига қараб уларни шартли равишда қуйидаги турларга ажратиш мумкин: тармоқ қуртлари, Троя дастурлари ва компьютер вируслари, мантиқий бомбалар. Алгоритм хусусиятларига кўра хилма-хил бўлгани учун вирусларни таснифлаш қийин. Шу билан бирга, диск файллари ва секторлари ичидагиларни ўзгартириб юборувчи паразитларга хос вирусларни ва компьютер манзилларини ҳисоблаб топиб, уларга ўз нусхаларини ёзиб қўювчи компьютер тармоқлари бўйлаб тарқаладиган репликаторларни (қуртларни) ажратиш мумкин. Паразитларга хос вирусларни топиш ва йўқ қилиш осон, репликаторлар эса топиш ва ҳимоя қилишнинг мураккаброқ ва мукаммалроқ воситаларини талаб қилади.

Зиён келтирувчи дастурларнинг ОКОТда йўл қўйган хатолари принципларини ўрганиш муайян компьютернинг очиқ кодли операцион тизими бир ёки бир нечта заиф томонларга эга бўлсагина ушбу дастурлар унга кира олишини кўрсатди. Шу сабабли компьютерларга, шу жумладан ОКОТга ҳужумлар беш босқичда амалга оширилади: ўрганиш, татбиқ, сақланиш, тарқалиш, парализация. Ҳужумнинг дастлабки икки босқичи аниқлаш нуқтаи назаридан энг мураккаби ҳисобланади. Охирги учта босқич ёмон ниятли ҳаракатларнинг чекланган миқдорига эга ва шу сабабли нисбатан оддий воситалар билан топилади.

Зиён келтирувчи дастурлар таъсиридан ОКОТни ҳимоя қилишнинг самарали усулларидан бири изоляция қилиш усули ҳисобланади. Тизим ресурсларига қилинган мурожаатларни таҳлил қилиш усули бўйича изоляция усудлари хавфсизлик сиёсати, сигнатуралар ва статистик маълумотларга асосланган уч гуруҳга бўлинади. Ҳар бир ушбу усулларнинг камчиликларига (мураккаблигига, янглиш ишлаб кетишига) қарамай, уларни комплекс қўллаш янги ва номаълум хавфларни аниқлаш ва зиён келтирувчи дастурлар таъсиридан ОКОТни ҳимоя қилишнинг самарадорлигини ошириш имконини беради.

Хавфларнинг янги, аввал номаълум бўлган турларининг пайдо бўлиши ахборот хавфсизлигидаги жараёнларнинг ўзига хос хусусиятларидан бири ҳисобланади. Қатъий расмий тартиб-таомиллар билан уларни топиш ва йўқ қилиш талаб қилинган даражада самарали ҳимоя билан таъминламайди. Шу сабабли хавфнинг бундай турларини топиш учун Soft Computing (Юмшоқ ҳисоб-китоблар) интеллектуал технологиясининг эксперт тизимлари, продукцион қоидалари, нейротармоқ моделлари ва бошқа воситаларидан

фойдаланиб, эвристик усуллар, алгоритм моделлари ва дастурларини ишлаб чиқиш имкониятларини ўрганиш мақсадга мувофиқдир.

Иккинчи бўлимда зиён келтирувчи дастурлар таъсирини блокировкалаш усуллари ва моделлари келтирилган.

ОКОТга зиён келтирувчи дастурлар ва ресурслар иловаларини изоляция қилиш принципини қўллашга, шунингдек хавфсизлик қоидалари, ҳужумларни аниқлашнинг статистик усуллари ва сигрнатур усулларга асосланган очиқ кодли операцион тизимларни ҳимоя қилишнинг концепцияси таклиф этилди. Ушбу усуллардан комплекс фойдаланиш ОКОТ ҳимоясининг юксакроқ самарадорлигини таъминлайди.

ОКОТ ахборот хавфсизлиги жараёнларини таҳлил қилишда келиб чиқадиган тизим зиддиятларини аниқлаш ва йўқ қилиш учун ихтиро масалалари назарияси асосида тизим тузилмасининг зиддиятли хусусиятларини ажратиш имкони пайдо бўлди. Натижада кейинчалик тизим ишини тақсимлаш ва мақбуллаштириш орқали изоляция жараёнини (иловаларнинг) дастур таъсирини изоляция қилишга ва тизим ресурсларини изоляция қилишга ажратиш таклиф этилди.

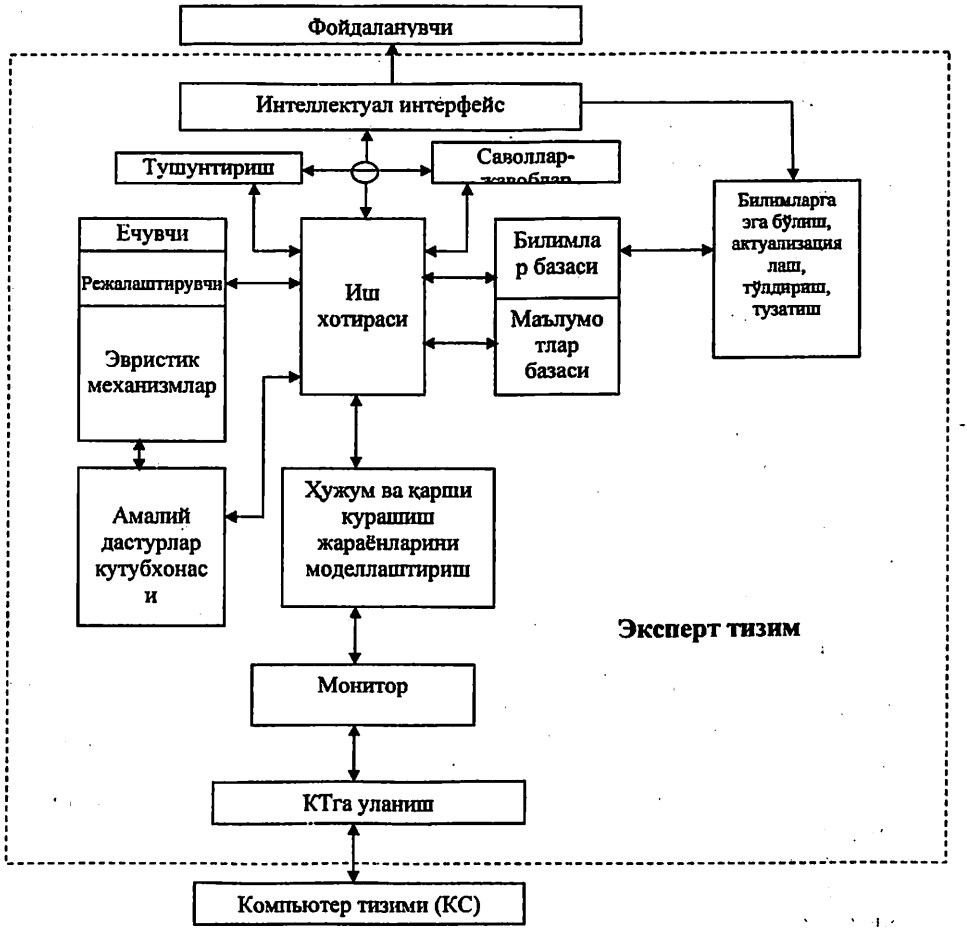
Зиён келтирувчи дастурлар таъсирини блокировкалашнинг модификацияланган тизими эксперт тизим (ЭТ) тузилмаси шаклида кўрсатилди. Қарорларлар ҳосил қилиш ва қабул қилиш учун ЭТда "Ҳал қилувчи", "Режалаштирувчи", "Эвристик механизмлар (мантиқий фикрлар ва хулосалар)" назарда тутилди. Ушбу кичик тизимлар учун зарур бўлган ахборот билимлар ва маълумотлар базасидан келиб тушади. Улар хавфсизликнинг барча қоидалари, шунингдек зиддият ҳавфлари ва воситалари тўғрисида билимларни акс эттирувчи продукцион қоидалардан иборат. Бу кичик тизимлар ОКОТ ахборот хавфсизлиги тизимининг ядросини ташкил этади. Блокировкалашнинг таклиф этилган ЭТ тузилмаси реал вақтда ОКОТ ахборот хавфсизлиги вазифаларини ҳал қилиш имконини беради.

Зиён келтирувчи дастурларнинг ва улар амалга оширадиган ҳужумларнинг янги, номаълум турлари пайдо бўлаётган шароитда эвристик усуллар ва уларни аниқлаш воситалари самарали ҳисобланади. Шу мақсадда хавф турлари ва улардан ҳимояланиш воситалари тўғрисидаги билимларнинг продукцион модели ишлаб чиқилди. Бу моделлар E1, E2, ... En эвристик продукцион қоидаларнинг мажмуи шаклида эксперт тизимининг билимлар базасида тақдим этилади. Ушбу қоидалар экспертлар хулосалари асосида ҳосил қилинган ва ахборот хавфсизлиги жорий ҳолати турини акс эттиради, компьютер тизими ишлаётган вақтда пайдо бўладиган рўйхатга олинадиган белгиларга мос келади (1-расм).

Зиён келтирувчи дастурлар иловаларини изоляция қилиш учун изоляция механизмидан фойдаланувчи усул таклиф этилди, унинг ички тузилиши изоляция, бошқарув ва хотира тизимларидан иборат. Мазкур тизимлар ўзаро алоқаси хусусияти иловаларни изоляция қилиш механизмларини бажарувчи алгоритмлар тузилиши хусусиятини белгилайди.

ОКОТни бошқарувчи ресурсларни изоляция қилиш усули қуйидаги яратувчи ресурсларни изоляция қилишни назарда тутади: қаттиқ диск секторлари, кириш параметри сифатида файл номига эга файллар билан ишлайдиган функцияларни тутиш ва қайта йўналтириш орқали файл тизимлари. Изоляция қилинадиган ресурслар учун хотира майдонларини ажратиш учун икки усул таклиф этилди: ҳимоя қилинадиган бўлим ҳажмига тенг дискдан жой бир марта ажратиш; зарур бўлганда хотира майдонларини ажратиш.

Ушбу усулларнинг амалга оширилиши излаш ва маълумотлар танлашнинг алоҳида алгоритмларини ишлаб чиқишни назарда тутади.



1-расм. Зиён келтирувчи дастурлар таъсирини блокиорвкаловчи ЭТ тузилиши

ЭТда кўриб чиқилган турининг тегишли қоидалари занжирини таҳлил қилиш асосида бир қарорга келинади. Бу қоидалар ЭТ билимлар базасида сақланади.

Диссертация ишининг **учинчи бўлимида** зиён келтирувчи дастурлардан очиқ кодли операцион тизимларни ҳимоя қилиш алгоритмлари келтирилган.

Қайта ишлаш учун изоляция объектларини бўлиш ҳақидаги ёндашувдан келиб чиққан ҳолда иловалар даражасида ва компьютер тизими ресурслари даражасида изоляция алгоритмлари ажратилди. Қуйида ёзиш учун файлни очиш операциясини изоляция қилиш алгоритми таърифи келтирилган:

- реал файл номи бўйича изоляция қилинган файл номини олиш;
- изоляция қилинган жойда файл борлигини текшириш;
- агар файл изоляция қилинган жойда бор бўлса, у ҳолда файлни очиш функциясини изоляция қилинган жойга қайта йўналтириш ва алгоритмдан чиқиш;
- агар изоляция қилинган жойда бўлмаса, у ҳолда реал жойда файл борлигини текшириш;
- агар файл реал жойда бор бўлса, у ҳолда уни изоляция қилинган жойга кўчириш ва у ерга файлни очиш функциясини йўналтириш, сўнгра алгоритмдан чиқиш;
- агар файл реал жойда бўлмаса, у ҳолда алгоритмдан чиқиш.

Файлни ўчириш операциясини изоляция қилиш алгоритми қуйидаги қадамлардан иборат:

- реал файл номи бўйича изоляция қилинган файл номини олиш;
- изоляция қилинган жойда файл борлигини текшириш;
- агар файл изоляция қилинган жойда бор бўлса, у ҳолда файлни ўчириш функциясини чақириш, сўнгра мазкур файлни масофавий файл деб белгилаш ва алгоритмдан чиқиш;
- агар файл изоляция қилинган жойда бўлмаса, у ҳолда реал жойда файлнинг борлигини текшириш;
- агар файл реал жойда бор бўлса, у ҳолда уни изоляция қилинган жойда масофавий деб белгилаш ва алгоритмдан чиқиш;
- агар файл реал жойда бўлмаса, у ҳолда алгоритмдан чиқиш.

Қуйида "ёзувни қайта йўналтириш" режимида секторга ёзиш операциясини изоляция қилишнинг алгоритми келтирилади:

- ёзиладиган сектор манзили ҳимоя қилинадиган манзиллар диапозонига киришини текшириш;
- агар кирса, у ҳолда мазкур секторни изоляция қилинган жойга (кэшга) ёзиш, индекс ахборотни янгилаш ва алгоритмдан чиқиш;

агар кирмаса, у ҳолда секторни оддий тарзда ёзиш ва алгоритмдан чиқиш.

Ёзувни қайта йўналтириш режимида секторни ўқиш операциясини изоляция қилиш алгоритми қуйидаги тарзда таърифланади:

• сектор ўқиладиган манзил ҳимоя қилинадиган манзилга киришини текшириш;

• агар кирмаса, у ҳолда секторни оддий ўқиш операциясини бажариш ва алгоритмдан чиқиш;

• агар кирса, у ҳолда мазкур сектор изоляция қилинган жойда жойлашганини текшириш;

• агар сектор изоляция қилинган жойда жойлашган бўлса, у ҳолда уни ўқиш ва алгоритмдан чиқиш;

• агар сектор изоляция қилинган жойда бўлмаса, у ҳолда секторни оддий ўқиш операциясини бажариш ва алгоритмдан чиқиш.

Ўзгаришлар изоляция қилинган кэшга қайта йўналтирилиши кўриб чиқилган алгоритмларнинг ўзига хос хусусияти ҳисобланади.

Сўнгра "ёзишда кўчириш" режимида секторга ёзишни изоляция қилиш алгоритми келтирилади:

• ёзилаётган сектор манзили ҳимоя қилинадиган манзиллар диапазонига киришини текшириш;

• агар кирмаса, у ҳолда секторни оддий ёзиш операциясини бажариш ва алгоритмдан чиқиш;

• агар кирса, у ҳолда мазкур сектор изоляция қилинган сектордалигини текшириш;

• агар сектор изоляция қилинган жойда бўлса, у ҳолда секторни оддий ёзиш операциясини бажариш ва алгоритмдан чиқиш;

• агар сектор изоляция қилинган жойда бўлмаса, у ҳолда уни изоляция қилинган жойга кўчириш, индекс ахборотни янгилаш, секторни ёзиш операциясини бажариш ва алгоритмдан чиқиш.

Мазкур алгоритм кэшда фақат оригинал секторлар сақланишини бажаради, янги секторлар эса эскилари ўрнига ёзилади. Бу режимда фақат ёзиш операциясини ишлаб битириш керак, чунки ўқиш операцияси доимо реал муҳитга нисбатан бажарилади.

Образларни аниқлаш назарияси доирасида белгиланадиган таснифлаш алгоритмларидан фойдаланиш ҳужумларни аниқлашни ўз ичига оладиган ҳимоя тизими асосини ташкил этади. Таснифлаш алгоритмини бажарувчи тизим компоненти классификатор деб аталади. Мазкур компонент ҳимоя тизимининг самарадорлигини белгилаб берувчи унинг муҳим компоненти ҳисобланган туфайли, классификатор ва иловаларни изоляция қилиш механизми ўзаро алоқасини аниқлаш муҳим вазифа ҳисобланади. Қуйида иловаларни изоляция қилиш механизмини қўллашнинг мақсадга мувофиқлигини ва самарадорлигини баҳолаш ва унинг методикаси кўриб чиқилади.

Математик усуллар ёрдамида таснифлаш учун математик таснифлаш аппаратидан фойдаланиб, фойдаланиш мумкин бўлган объектнинг расмий таърифини киритиш зарур. Одатда объект белгиларининг вектори (сон хусусиятлари) бундай таъриф бўлиб хизмат қилади. Белгилар векторининг ҳар бир элементи объектнинг айрим хусусияти тўғрисида ахборот беради.

Ҳимоя тизимида ечимлар қуйидагича белгиланади: Y = {Норма, Тревога}, "Тревога" бирор-бир дастурнинг зарарли таъсирини ёки бирорта файлда вирус борлигини ифодалайдиган ҳолат аниқланганига мос келади, "Норма" эса бундай ҳолат аниқланмаганини англатади. Биз ўқитувчи (supervised learning) билан ўрганиш вариантини кўриб чиқамиз, унда классификаторни ўқитиш учун биз векторларнинг бир нечта {E} тўпламидан фойдаланишимиз мумкин, уларнинг ечимлар муҳитида қийматларидан бирига мансублиги улар учун маълумдир. Классификаторни ўқитиш учун машқ қилиш тўплами деб аталган махсус тайёрланган маълумотлардан фойдаланилади. Машқ қилиш тўпламида классификатор ўқитилганидан кейин олинган классификатор сифатини баҳолаш зарур.

Умумий ҳимоя тизими билан бирга ишлайдиган изоляция механизмлари ва алгоритмларининг самарадорлигини баҳолаш методикаси қуйидаги тартиб-таомилларни босқичма-босқич амалга оширишни назарда тутади:

- ахборот белгиларини ва таснифлаш алгоритмини танлаш;
- классификатор учун машқ тўпламини яратиш;
- машқ тўпламида классификаторни ўргатиш;
- классификатор учун тест тўпламини олиш;
- мантиқий изоляциядан фойдаланмай туриб, классификатор сифати хусусиятларини олиш;
- мантиқий изоляциядан фойдаланиб, классификатор сифати хусусиятларини олиш.

Самарадорликни баҳолаш тартибларини моделлаштиришнинг ишлаб чиқилган тизими иловалар кўрсатадиган зарарли таъсир турларини таснифлаш алгоритмларидан фойдаланишга асосланган. Бунда реал вақт режимида тизим хавфлари тўғрисида статистика тўпланади ва муайян мезонлар бўйича олинадиган ахборот таҳлили асосида тизимнинг ишлаши хусусияти тўғрисида қарорга келинади. Агар айрим иловаларнинг муомаласи зарарли деб тавсифланса, у ҳолда уни бажариш блокировкаланади, фойдаланувчи эса унинг ҳужуми тўғрисида хабардор этилади. ЭТ билимлар ва маълумот базасида тегишли қарорлар қабул қилингунича иловаларнинг (тизим блокларининг) нормал ишлаши (таъсири) эталонлари (ихтисослиги) тўғрисидаги ахборот олдиндан киритилади. Ушбу эталонлар билан тизимнинг жорий (амалдаги) ҳолати бўйича маълумотлар тенглаштирилади ва улар мос келмаганда уларни блокировкалаш (изоляция қилиш) тўғрисида қарор қабул қилинади.

Иловани изоляция қилиш самарадорлигини баҳолаш учун иловаларни изоляция қилиш механизми билан ва у сиз ишлайдиган классификаторнинг сифатли хусусиятларини ҳисоблаш ва тенглаштириш имконини берадиган эксперт тизимидан фойдаланиш таклиф этилади. Эксперт тизимига киришда олдинги қадамда олинган қийматларига эга тўплам берилади, чиқишида эса биринчи ва иккинчи турнинг хатолари қийматлари, шунингдек тизим самарадорлиги нисбати олинади.

Мазкур методикадан фойдаланиб, биз ҳимоя статистик тизимининг аниқ бир мисолида иловани изоляция қилиш механизмини қўллашнинг мақсадга мувофиқлиги тўғрисида хулоса қилишимиз мумкин.

Классификаторнинг сифат хусусиятлари қуйидагича билдирилади:

- K_d – аниқлаш ёки самарадорлик нисбати (классификаторнинг тўғри қарорлар қабул қилишга қодирлиги);
- K_{e1} – биринчи турнинг хатога йўл қўйиш эҳтимоли, (мақсадни ўтказиб юбориш);
- K_{e2} – иккинчи турнинг хатога йўл қўйиш эҳтимоли, (ёлғон тревога).

Мазкур параметрлар колган олти параметр базасида бир шаклга келтирилиши мумкин:

- D_i — W_s векторининг W_1 векторидан оғиш қиймати $D(w_s, w_1) > D_i$ га ўхшаш бўлиб, унда тизимнинг ишлаши зарарли деб таснифланади;
- D_s - W_s векторининг W_1 векторидан оғиш қиймати $D(w_s, w_1) => D_s$ га ўхшаш бўлиб, унда тизимнинг ишлаши шубҳали деб таснифланади;
- E_i – зарарли таъсир кўрсатилаётганидан дарак берувчи ҳолат;
- G_i – тизимнинг ишлаши зарарли экани ва W_s вектори W_1 векторидан $D(w_s,w_1) => D_j$ масофага оғаётгани ҳақидаги тахмин;
- G_s – тизимнинг ишлаши шубҳали экани ва W_s вектори W_1 векторидан $D_i => D(w_s,w_1) => D_s$ масофага оғаётгани ҳақидаги тахмин;
- G_n – тизимнинг ишлаши нормал экани ва W_s вектори W_1 векторидан $D(w_s, w_1) <= D_s$ масофага оғаётгани ҳақида тахмин.

Таърифланган параметрлардан фойдаланган ҳолда классификаторнинг сифатли хусусиятларини чиқарамиз.

$$K_d = \frac{p(G_i|G_i)\times p(G_i)}{p(G_i|G_i)\times p(G_i) + p(E_i|G_s)\times p(G_s) + p(E_i|G_n)\times p(G_n)} \quad (1)$$

$$K_{e1} = p(E_i|G_i) \quad (2)$$

$$K_{e2} = 1 - p(E_i|G_i) \quad (3)$$

Мазкур формулалар эксперт тизимининг оддий модели бўлиб, унинг базасида таснифлашнинг турли тизимларини солиштириш мумкин.

Гарчи K_{e1} биринчи тур хатоси камайса-да, D_i қийматининг камайиши ҳисобига K_d параметрининг яхшиланиши K_{e2} иккинчи тур хатосининг ошишига олиб келиши муқаррарлиги мазкур моделнинг ўзига хос жиҳати ҳисобланади. Ва аксинча, агар D_i қиймати ошса, у ҳолда K_d параметри ва K_{e2} иккинчи тур хатоси камаяди, K_{e1} биринчи тур хатоси эса ортади.

Шу сабабли K_d тизимининг самарадорлиги ва биринчи ва иккинчи тур хатолари қийматлари ўртасида муроса ўрната оладиган D_i қийматини эмпирик йўл билан топиш таснифлаш тизими учун муҳимдир.

Агар таснифлаш тизими тизим номаълум ёки шубҳали ишлаганда ёқиладиган мантиқий изоляция механизми бирга ишласа, у ҳолда тизимнинг эксперт тизими модели қуйидагича кўриниш олади:

$$K_d = \frac{p(E_i|G_i)\times p(G_i)\times p(E_i|G_s)\times p(G_s)}{p(E_i|G_i)\times p(G_i)+p(E_i|G_s)\times p(G_s)+p(E_i|G_n)\times p(G_n)} \quad (4)$$

$$K_{e1} = p(E_i|G_n) \quad (5)$$

$$K_{e2} = 1 - p(E_i|G_n) \quad (6)$$

Олинган модулни аввалгиси билан таққослаб, шуни қайд этиш мумкинки, таснифлашнинг бирорта мавжуд тизимига мантиқий изоляция механизми қўшилса ҳамда D_i ва D_s қийматлари тўғри танланса, параметр бўйича самарадорлик ошади ва хато қийматлари камаяди. Бироқ доим ҳам бундай бўлавермаслиги мумкин, чунки классификатор сифати хусусиятлари кўп жиҳатдан аниқ тест сиёновларига боғлиқ.

Эксперт тизимининг таклиф этилган тузилмаси классификатор хусусиятларини ҳисоблаб чиқиш билан бирга изоляция механизмларини қўллаш ва уларни қиёслаш имконини беради. Бундай комплекс баҳолар асосида изоляция механизмлари ва алгоритмларининг самарадорлигини баҳолаш бўйича аниқроқ қарорлар қабул қилиш имконияти пайдо бўлади.

Ҳисоблаш эксперименти натижалари изоляция алгоритмларида қўлланиладиган таснифлашнинг таклиф этилган тартиб-таомиллари юксак даражада самарадор эканини кўрсатди.

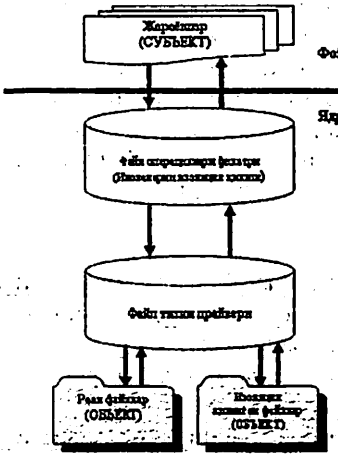
Тўртинчи бўлимда иловалар ва тизимлар даражасида изоляция қилиш алгоритмларини амалга оширувчи дастурлар келтирилган. Шу билан бирга очиқ кодли операцион тизимда иловаларни изоляция қилишнинг дастурий воситаларини экспериментал текшириб, ҳимоя дастурий воситаларидан фойдаланиш бўйича тавсиялар берилган.

Зиён келтирувчи дастурлардан ОКОТни ҳимоя қилиш дастурларининг ишлашини ташкил этиш схемаси ҳимоя воситасининг икки даражаси драйверлари борлигини назарда тутади: файл тизимини фильтрлаш драйверлари ва диск операцияларини фильтрлаш драйверлари. Бу драйверлар зарарли функцияларни тутиш, изоляция қилиш ва изоляция қилинган жойга қайта юбориш тартиб-таомилини амалга ошириш имконини беради (2,3-расм).

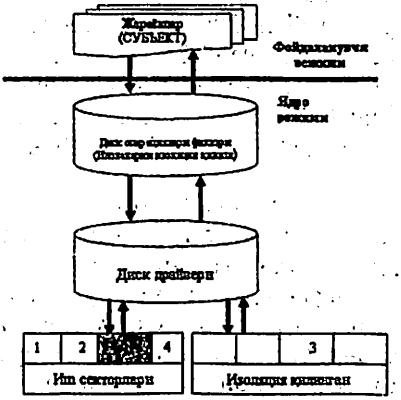
ОКОТдаги иловаларни изоляция қилиш дастурий воситаларининг ишлашга лаёқатини экспериментал текширувдан ўтказиш:

- ОКОТ ядроси даражасида иловаларни изоляция қилиш тартиб-таомилларини бажариш;
- фойдаланишни назорат қилиш тизимларида изоляция механизмидан фойдаланиш, ҳужумларни ва антивирус сканерларни аниқлаш;
- мавжуд ҳимоя тизимлари билан бирга изоляция механизмларидан фойдаланиш;

- иловалар ва ресурсларни изоляция қилиш дастурий воситаларининг самарадорлигига эришиш имкониятини кўрсатди.



2-расм. Файл операциялари фильтри даражасида иловаларни изоляция қилиш



3-расм. Диск операциялари фильтри даражасида изоляция қилиш

Иловаларни изоляция қилиш дастурини амалий баҳолаш унинг функцияларини ва иловаларни изоляция қилишнинг тизим самарадорлигига кўрсатган таъсирини миқдорий баҳолашни экспериментал текширувдан ўтказишдан иборат.

Амалий баҳолаш бажариш вақти кийматлари таърифидан иборат:

- изоляция ўчирилганда 20 МБ файлни ўқиш, ёзиш ва кўчириш операциялари;

- "Ёзаётганда қайта йўналтириш" муҳитида изоляция қилаётганда ушбу операциялар;

- "Ёзаётганда нусха кўчириш" муҳитида изоляция қилишда ушбу операциялар ва изоляция вақтида амалга оширилган ўзгартиришларни қўллаш функцияларининг ишга лаёқатлилигини текшириш.

Тест ўтказишда UzMOT (Uzbek Milliy Operatsion Tizimi) очиқ кодли операцион тизими, Intel Celeron процессорли, 1,73 ГГц частотали ва 1024 МБ оператив хотирали компьютердан фойдаланилди.

Тестларни ўтказиш вақти тестни бошлаш ва тест бажарилгандан кейин белгиланадиган вақт фарқини ҳисоблаш йўли билан аниқланди. Тестларнинг миқдорий натижалари 1-жадвалда келтирилган.

1-жадвал

20 МБ ҳажмли файлни тестдан ўтказиш натижалари

Ҳаракат	Тест синовидан ўтказиш	Вақт, мс
Ёзиш	Изоляциясиз тест	1484
	Ёзаётганда қайта йўналтиришни текшириш	1506
	Ёзаётганда кўчиришни текшириш	3052
Ўқиш	Изоляциясиз тест	1013
	Ўқаётганда қайта йўналтиришни текшириш	1022
	Ёзаётганда кўчиришни текшириш	1011
Кўчириш	Изоляциясиз тест	2682
	Қайта йўналтирилганда кўчиришни текшириш	2803
	Ёзаётганда кўчиришни текшириш	2951

Кўриб чиқилган ҳимоя технологиясига мослашган дастур комплекси ишлаб чиқилди. Қуйидаги компонентлар дастур комплекси таркибига киради: детекторлар каталоги, вирусларни тутиш дастури, вакцинация дастури, зиён келтирувчи дастурлар ва уларнинг хусусиятлари тўғрисида билимлар ва маълумотлар базаси, ҳимоянинг резидент воситалари. Дастурларни ўрганишдан ҳимоя қилиш самарадорлигини ошириш учун ҳимоя қилишга қаратилган хавфсизликнинг қўшимча функциялари дастурга киритилди.

ХУЛОСА

Диссертация ишида қайд этилган асосий илмий натижалар қуйидаглардан иборат:

1. Очиқ кодли операцион тизимларда зиён келтирувчи дастурларга қарши курашиш тадқиқ этилди. Зиён келтирувчи дастурларнинг очиқ кодли операцион тизимларга хавф солувчи турлари ва хавфлари кўриб чиқилди.

Зиён келтирувчи дастурларнинг зарарли таъсирини изоляция қилишнинг мавжуд усуллари шарҳланди.

2. Номаълум шароитларда очиқ кодли операцион тизимларни ҳимоя қилиш, тизим иловалари ва ресурсларини зиён келтирувчи дастурлардан изоляция қилиш принципига асосланган тизимдан фойдаланиш концепцияси таклиф этилди.

3. Ихтиро масалаларини ҳал қилиш назариясидан ва зиён келтирувчи дастурлар таъсирини изоляция қилиш принципидан фойдаланишга асосланган зиён келтирувчи дастурлар таъсирини блокировкалашнинг модификацияланган усули ишлаб чиқилди. ОКОТ ядросининг зиён келтирувчи дастурлардан ҳимоя қилиш воситалари тўғрисидаги билимларнинг продукцион модели яратилди. Зиён келтирувчи дастурлар таъсирини блокировкалашнинг ЭТ функционал тузилмаси ишлаб чиқилди. Бу ўз навбатида реал вақт ичида мустақил қарор қабул қилиш ва билимлар базасида янги қоидалар пайдо бўлишига олиб келди.

4. Иловалар ва тизим даражасида изоляция қилиш алгоритмлари ҳамда таснифлаш алгоритми қурилди. Таклиф этилган методикалардан фойдаланган ҳолда ушбу алгоритмларнинг самарадорлигига баҳо берилди. Натижада зиён келтирувчи дастурларни аниқлаш имконияти ва тезлигининг ошишига эришилди.

5. Диск операцияларни фильтрлаш даражасида иловаларни изоляция қилишнинг дастурий воситалари ишлаб чиқилди. Зиён келтирувчи дастурларга қарши курашувчи воситалар экспериментал текширувдан ўтказилди, унинг натижаси уларнинг ишлашга қодирлигини ва реал шароитларда уларни қўллаш мумкинлигини кўрсатди. Дастурий воситалар ОКОТ ядроси даражасида яратилганлиги боис ОКОТнинг ишлаш тезлигига таъсир қилмаслигига эришилди.

6. Зиён келтирувчи дастурлардан ОКОТни ҳимоя қилувчи дастурий воситалар ISP «Dostlink» МЧЖда амалда татбиқ этилди. Амалдаги татбиқ шуни кўрсатдики, яратилган моделлар, алгоритмлар дастурий воситаларнинг ишлаш тезлигини ва самарадорлигини ошириб, ишлаб чиқилган ЭТ функционал тузилмаси эса номаълум бўлган зиён келтирувчи дастурларни аниқлаш ва блокировка қилишга эришди.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ

1. С.С.Қосимов, Жон Жей Санг, Ким Сунг Су, Н.Э.Махаматов, О.Н.Джураев, Д.Н.Рахматов, С.Н.Беков. Uz-booyo 1.0 operatsion tizimi // Ўзбекистон Республикаси Давлат патент идораси. Гувоҳнома № DGU 01547. 19.06.2008 й.
2. С.С.Қосимов, Д.Н.Рахматов, М.Я.Мансурова. Очиқ кодли операцион тизимларни – i18n/l10n махаллийлаштириш, қўллаш ва созлаш // Вестник ТУИТ. – Ташкент, 2009. - № 2. – С. 15-18.

3. С.С.Қосимов, Д.Н.Рахматов, Ю.С.Алиева. Очиқ кодли операцион тизимларда SourseForge тармоқ лойихасида жамият структурасини қўлланилиши // Вестник ТУИТ. – Ташкент, 2009. - № 3. – С. 10-14.
4. Д.Н.Рахматов. Problems of safety of information systems // Международная конференция. Актуальные проблемы прикладной математики и информационной технологий – Аль Хорезми 2009. – Ташкент, 2009. – С. 143-144.
5. Д.Н.Рахматов. Операцион тизимларда ахборот хавфсизлигини пароллар ёрдамида ташкиллаштириш // Республиканский семинар. Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения. – Ташкент, 2009. – С. 59-61.
6. Д.Н.Рахматов. Modern technology to detect and prevent attacks // Международная научная конференция. Проблемы развития информационно-коммуникационных технологий и подготовка кадров. – Ташкент, 2009. – С. 140-144.
7. С.С.Қосимов, Д.Н.Рахматов. A comparison mechanism of security to authentifications and identifications on operating systems Linux and Solaris // Сборник трудов международной научной конференции. Проблемы развития информационно-коммуникационных технологий и подготовки кадров. – Ташкент, 2009. – С. 110-114.
8. С.С.Қосимов, Д.Н.Рахматов. Методы защиты информационных систем от вирусных угроз // Вестник ТУИТ. – Ташкент, 2010. - № 1. – С. 7-10.
9. С.С.Қосимов, Ким Сунг Су, Н.Э.Махаматов, О.Н.Джураев, Д.Н.Рахматов, Р.И.Рахимов, О.Нуриддинов. UzMOT 1.0 operatsion tizimi // Ўзбекистон Республикаси Давлат патент идораси. Гувоҳнома № DGU 01899. 04.03.2010 й.
10. Д.Н.Рахматов. Построение продукционной модели знаний о вирусных угрозах и оценка типа вирусной угрозы // Вестник ТУИТ. – Ташкент, 2010. - № 2. – С. 39-42.
11. С.С.Қосимов, Д.Н.Рахматов. Алгоритмы изоляции логических и физических объектов от вредоносных программ // 4-я IEEE Международная конференция по использованию информационно-коммуникационных технологий - AICT2010. – Ташкент, 2010. – С. 289-293.
12. С.С.Қосимов, Д.Н.Рахматов, Д.Мадусмонов. Технологии блокирования поведения вредоносных программ // 4-я IEEE Международная конференция по использованию информационно-коммуникационных технологий - AICT2010. – Ташкент, 2010. – С. 349-353.

Техника фанлари номзоди илмий даражасига талабгор Рахматов Дилшод Нигматиллаевичнинг 05.13.19 – Ахборотларни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги ихтисослиги бўйича "Очиқ кодли операцион тизимларга зиён келтирувчи дастурлардан ҳимоялашнинг дастурий воситалари" мавзусидаги диссертациясининг

РЕЗЮМЕСИ

Таянч (энг муҳим) сўзлар: очиқ кодли операцион тизимлар, билимлар базаси, қамал қилиш, изоляциялаш, классификатор, зиён келтирувчи дастурлар, эксперт тизимлар, ахборот хавфсизлиги, рухсатсиз фойдаланиш.

Тадқиқот объектлари: очиқ кодли операцион тизимларни зиён келтирувчи дастурлардан ҳимоя қилишнинг алгоритмлари ва дастурий воситалари.

Ишнинг мақсади: зиён келтирувчи дастурларни аниқлаш ва олдини олиш учун алгоритм ва дастурий воситаларни очиқ кодли операцион тизим ядроси даражасида ишлаб чиқиш.

Тадқиқот методлари: ахборот ҳимоясига хавф солувчи таҳдидларни аниқлаш усуллари, ихтиро масалаларини ечиш назарияси, эксперт тизим продукцион усуллари, алгоритмлар назарияси ва объектга мўлжалланган дастурлаш.

Олинган натижалар ва уларнинг янгилиги: ОКОТ ҳимояси концепциясига асосланган зиён келтирувчи дастурларни қамал қилишнинг модификацияланган усули ва алгоритмлари таклиф этилди; зиён келтирувчи дастурлардан ОКОТ ядросини ҳимоя қилиш воситалари тўғрисидаги кўникмаларнинг продукцион усули яратилди; иловалар даражасида зиён келтирувчи дастурларни изоляция қилишнинг моделлаштириш алгоритми ишлаб чиқилди; зиён келтирувчи дастурларни қамал қилиш ва изоляция қилишнинг эксперт тизими тузилмаси яратилди, унинг доирасида ҳимоя воситалари танлови бўйича реал вақтда қарорлар қабул қилиш методикаси таклиф этилди; ОКОТ ҳимоя тизимларига зиён келтирувчи дастурлар таъсирини қамал қилиш ва изоляция қилиш дастурлари ишлаб чиқилди.

Амалий аҳамияти: яратилган моделлар, алгоритмлар ва дастурий воситалар реал вақт ичида хавфни баҳолаш ва ҳимоялаш воситасини танлашга қарор қилувчи эксперт тизимларини яратади.

Татбиқ этиш даражаси ва иқтисодий самарадорлиги: диссертация ишининг илмий натижалари Тошкент ахборот технологиялари университетининг "Электрон тижорат" ва "Ахборот хавфсизлиги" кафедраларининг ўқув жараёнига татбиқ этилди, ҳамда амалий натижалари МЧЖ ISP «DosTlink» Интернет сервис провайдерда жорий этилди.

Қўлланиш (фойдаланиш) соҳаси: яратилган дастурий воситалар Linux операцион тизимини сервер сифатида фойдаланаётган корхоналарда очиқ кодли операцион тизимларга зиён келтирувчи дастурлардан ҳимоялаш учун қўлланилади.

РЕЗЮМЕ

диссертации Рахматова Дилшод Нигматиллаевича на тему "Программные средства защиты от вредоносных программ операционных систем с открытым кодом" на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Ключевые слова: операционные системы с открытым кодом, база знаний, блокировка, изоляция, классификатор, вредоносные программы, экспертная система, безопасность информации, несанкционированный доступ.

Объекты исследования: алгоритмы и программные средства защиты операционных систем с открытым кодом от вредоносных программ.

Цель работы: разработка алгоритмов и программных средств обнаружения и предотвращения вредоносных программ на уровне ядра ОСОК.

Методы исследования: методы обнаружения угроз защиты информации, теория и методы изобретательских задач, методы продукционных экспертных систем, теория алгоритмов, объектно-ориентированное программирование.

Полученные результаты и их новизна: предложены модифицированный метод и алгоритм блокирования вредоносных программ, основанные на предложенной концепции защиты ОСОК; построена продукционная модель знаний о средствах защиты ядра ОСОК от вредоносных программ; разработан алгоритм моделирования изоляции вредоносных программ на уровне приложений; построена структура экспертной системы блокирования и изоляции вредоносных программ, в рамках которой предложена методика принятия решений в реальном времени по выбору средств защиты; разработаны программы блокирования и изоляции поведения вредоносных программ для систем защиты ОСОК.

Практическая значимость: разработанные модели, алгоритмы, программные средства позволяют строить экспертные системы для принятия решений по оценке угроз и выбору средств защиты в реальном масштабе времени.

Степень внедрения и экономическая эффективность: полученные результаты используются в учебном процессе на кафедрах «Электронная коммерция» и «Информационная безопасность» Ташкентского университета информационных технологий, а также внедрены и использованы в Интернет сервис провайдере ООО ISP «DosTlink».

Область применения: разработанные программные средства могут быть применяться для защиты операционных систем с открытым кодом от вредоносных программ в организациях использующие сервера на основе ОС Linux.

RESUME

Thesis of Rahmatov Dilshod on the scientific degree competition of the doctor of philosophy in technical on specialty 05.13.19 – "Methods and systems of protecting information, information security" subject: "Software protection against malicious programs operating systems with open source"

Key words: operating systems with open source software, knowledge base, blocking, insulation, classifier, malicious software, expert system, information security, unauthorized access.

Subjects of the inquiry: algorithms and security software operating systems with open source (OSOS) software against malicious software.

Aim of the inquiry: development of algorithms and software tools to detect and prevent malicious software at the core of OSOS.

Methods of inquiry: methods for detection of threats to information security, theory and methods of inventive problem solving, methods of production of expert systems, theory of algorithms, object-oriented programming.

The results achieved and their novelty: a modified method and algorithm for blocking malicious programs based on the proposed concept of protection OSOS; built with production of knowledge about anti-nuclear OSOS from malicious programs designed an algorithm that simulates malware insulation level applications built structure of expert system to block and isolate malicious programs, within which the technique of making real-time by choice of remedy developed programs to block and isolate malicious behavior for protection systems OSOS.

Practical value: developed models, algorithms, software tools allow to build expert systems for decision-making to assess the threat and the choice of remedies in real time.

Degree of embed and economic effectivity: The results are used in the learning process in the departments "E-commerce" and "Information Security" Tashkent University of Information Technology, as well as implemented and used in the Internet Service Provider Ltd ISP «DosTlink».

Sphere of usage: developed software tools can be used to protect operating systems, open source software against malicious programs in organizations using servers based on Linux.

Босишга рухсат этилди. 29.09.2011 й.
Босма табоқ 1,375. Адади 100. Буюртма № 30/09.
“Yosh kuch press matbuoti” МЧЖ босмахонасида чоп этилди.
Манзил: Тошкент, Сўгалли ота, 5.